Dialogic® BorderNet™ 4000 Session Border Controller (SBC)

Maintenance and Troubleshooting Guide

October 2012 64-0549-04

www.dialogic.com

Copyright and Legal Notice

All contents of this document are furnished for informational use only and are subject to change without notice and do not represent a commitment on the part of Dialogic Inc. and its affiliates or subsidiaries ("Dialogic"). Reasonable effort is made to ensure the accuracy of the information contained in the document. However, Dialogic does not warrant the accuracy of this information and cannot accept responsibility for errors, inaccuracies or omissions that may be contained in this document.

INFORMATION IN THIS DOCUMENT IS PROVIDED IN CONNECTION WITH DIALOGIC® PRODUCTS. NO LICENSE, EXPRESS OR IMPLIED, BY ESTOPPEL OR OTHERWISE, TO ANY INTELLECTUAL PROPERTY RIGHTS IS GRANTED BY THIS DOCUMENT. EXCEPT AS PROVIDED IN A SIGNED AGREEMENT BETWEEN YOU AND DIALOGIC, DIALOGIC ASSUMES NO LIABILITY WHATSOEVER, AND DIALOGIC DISCLAIMS ANY EXPRESS OR IMPLIED WARRANTY, RELATING TO SALE AND/OR USE OF DIALOGIC PRODUCTS INCLUDING LIABILITY OR WARRANTIES RELATING TO FITNESS FOR A PARTICULAR PURPOSE, MERCHANTABILITY, OR INFRINGEMENT OF ANY INTELLECTUAL PROPERTY RIGHT OF A THIRD PARTY.

Dialogic products are not intended for use in certain safety-affecting situations. Please see http://www.dialogic.com/company/terms-of-use.aspx for more details.

Due to differing national regulations and approval requirements, certain Dialogic products may be suitable for use only in specific countries, and thus may not function properly in other countries. You are responsible for ensuring that your use of such products occurs only in the countries where such use is suitable. For information on specific products, contact Dialogic Inc. at the address indicated below or on the web at www.dialogic.com.

It is possible that the use or implementation of any one of the concepts, applications, or ideas described in this document, in marketing collateral produced by or on web pages maintained by Dialogic may infringe one or more patents or other intellectual property rights owned by third parties. Dialogic does not provide any intellectual property licenses with the sale of Dialogic products other than a license to use such product in accordance with intellectual property owned or validly licensed by Dialogic and no such licenses are provided except pursuant to a signed agreement with Dialogic. More detailed information about such intellectual property is available from Dialogic's legal department at 9800 Cavendish Blvd., 5th Floor, Montreal, Quebec, Canada H4M 2V9. **Dialogic encourages all users of its products to procure all necessary intellectual property licenses required to implement any concepts or applications and does not condone or encourage any intellectual property infringement and disclaims any responsibility related thereto. These intellectual property licenses may differ from country to country and it is the responsibility of those who develop the concepts or applications to be aware of and comply with different national license requirements.**

Dialogic, Dialogic Pro, Dialogic Blue, Veraz, Brooktrout, Diva, Diva ISDN, Making Innovation Thrive, Video is the New Voice, VisionVideo, Diastar, Cantata, TruFax, SwitchKit, SnowShore, Eicon, Eiconcard, NMS Communications, NMS (stylized), SIPcontrol, Exnet, EXS, Vision, PowerMedia, PacketMedia, BorderNet, inCloud9, I-Gate, ControlSwitch, NaturalAccess, NaturalCallControl, NaturalConference, NaturalFax and Shiva, among others as well as related logos, are either registered trademarks or trademarks of Dialogic Inc. and its affiliates or subsidiaries. Dialogic's trademarks may be used publicly only with permission from Dialogic. Such permission may only be granted by Dialogic's legal department at 9800 Cavendish Blvd., 5th Floor, Montreal, Quebec, Canada H4M 2V9. Any authorized use of Dialogic's trademarks will be subject to full respect of the trademark guidelines published by Dialogic from time to time and any use of Dialogic's trademarks requires proper acknowledgement.

The names of actual companies and products mentioned herein are the trademarks of their respective owners.

This document discusses one or more open source products, systems and/or releases. Dialogic is not responsible for your decision to use open source in connection with Dialogic products (including without limitation those referred to herein), nor is Dialogic responsible for any present or future effects such usage might have, including without limitation effects on your products, your business, or your intellectual property rights.

Table of Contents

About this Publication 6
Related Documentation 6

Overview 7

Diagnostics 8
Alarms 8
Alarm History 8
Categories 9
Alarm Customization 10
Reporting Pending Alarms 11
Reporting Alarm History 13

Statistical Reports 14
Reporting Ethernet Links 15
Peer Statistics 16
Reporting Summary 16
Reporting Peer Packet Statistics 17
Reporting Incoming Sessions 18
Reporting Outgoing Sessions 19
Interface Statistics 20
Reporting Summary 20
Reporting Incoming Sessions 21
Reporting Outgoing Sessions 22
System Statistics 23
Reporting Packet Statistics 23
Reporting Incoming Statistics 24
Reporting Outgoing Sessions 25

Tracing 26
Downloading the Trace Plug-in 26
Connecting to the BorderNet 4000 SBC from Wireshark 27
Recording Profiles 29
Message Based Capture Filters 29
Interface based capture filters 30
Session Tracing 31
Media Capture 31

System Status 32
Reporting ACL Status 32
Reporting IP Route Status 33

Real-Time Status and Performance 34
Alarms 34
Dashboard 34
Memory 35
CPU Usage 36
Storage and Temperature 36
Alarm Severity, Packet Drop, License Capacity 36
System Performance 37
Platform Status 38
Session Link Utilization 39
Reporting CPU Utilization 39

Software Management 41
Displaying Software Information 41
Uploading a New Software Release 42
Upgrading Software 43
Rolling Back Software 44
Restoring and Backing Up Configuration Data 44
Starting the Backup 45
Restoring the Backup 45
Downloading the Backup 45
Deleting the Backup 45
Uploading the Backup 45
Audit Logs 46
Viewing Audit Logs 47
Troubleshooting 49
Alarms 49

Revision History

Revision	Release date	Notes
64-0549-03	September 2012	Release 2.1
64-0549-02	July 2012	Release 2.0
64-0549-01	March 2012	Controlled Introduction

Refer to www.dialogic.com for product updates and for information about support policies, warranty information, and service offerings.

About this Publication

The *Dialogic® BorderNet™ 4000 SBC Maintenance and Troubleshooting Guide* provides the information that you need to operate the Dialogic® BorderNet™ 4000 SBC after it is installed, deployed, and configured.

The Dialogic® BorderNet™ 4000 SBC is also referred to herein as the "BorderNet 4000 SBC" and/or the "BorderNet 4000."

Related Documentation

- *Dialogic® BorderNet™ 4000 SBC Product Description*
- *Dialogic® BorderNet™ 4000 SBC Installation and Deployment Guide*
- *Dialogic® BorderNet™ 4000 SBC Configuration Guide*
- *Dialogic® BorderNet™ 4000 SBC Regulatory Notice*
- Dialogic® BorderNet™ 4000 SBC Field Replaceable Unit documents
    - Replacing a Fan Assembly
    - Replacing the Air Filter
    - Replacing a Power Supply

Overview

The BorderNet 4000 SBC contains a WebUI, which includes the following two modules that allow you to maintain your system:

- Diagnostics
- Software Management

The Monitor and Diagnostics module enables the following:

- Alarms
- Statistical Reports
- System Performance
- Tracing
- System Status

The Software Management module enables the following:

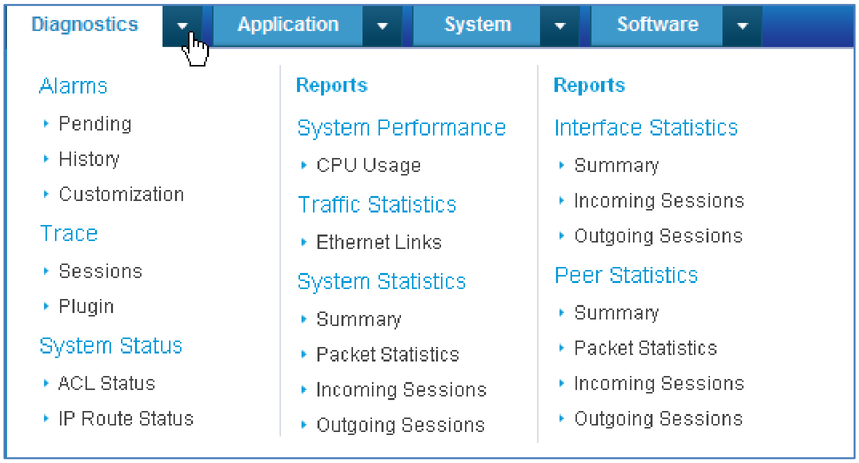
- Upgrading software
- Uploading new releases of software

Diagnostics

This section explains how to use the Monitor and Diagnostics module to maintain your BorderNet 4000 SBC including the following:

- alarms
- reports
- performance
- tracing
- system status

The procedures in this section are available from the Diagnostics menu below.



Alarms

The WebUI gathers and presents alarms as follows:

- Pending Alarm screen, which allows operators to view all pending alarms and to filter all pending alarms based on severity, category, time, and name.
- Alarm History screen, which allows operators to view all historical alarms and to filter alarms based on severity, name, category, time, reported object type and FDN.
- Alarm Customization screen, which enables operators to customize severity, to set whether to generate SNMP trap, whether to generate email notice on each individual alarm.

Alarms can be filtered by severity, category, time, and so forth. BorderNet 4000 SBC enables operators to change severity, generate an SNMP trap, or generate email notices for each individual alarm.

See also the Alarms section in the Troubleshooting chapter for listing of alarms and corrective actions.

Alarm History

Alarms from the last seven days are retained in the system (by default). Non-pending alarms older than seven days are purged every 24 hours.

Categories

The BorderNet 4000 SBC supports the following category of alarms:

- QoS
- Configuration
- HA
- License
- Peer
- Overload
- Hardware
- Network
- System
- Security
- Session

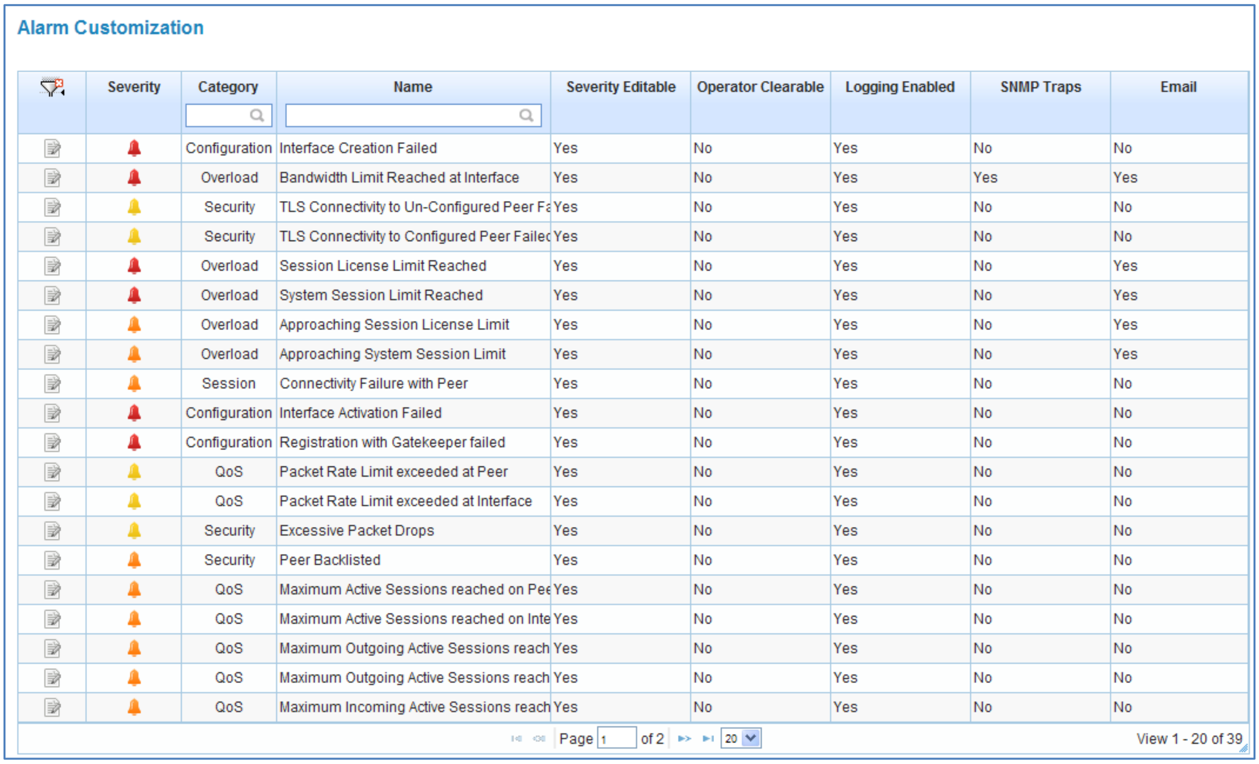
The following are the severity levels and the corresponding icon color:

- Critical 🔔(Red)
  Critical alarms are a subgroup of the major alarms. Critical alarms are issued when service has stopped and an immediate corrective action is required.
- Major 🔔 (Orange)
  A major alarm is raised when service affecting condition has developed and an immediate corrective action is required.
- Minor 🔔 (Yellow)
  A minor alarm condition is raised due to the existence of non-service affecting fault condition and that corrective action should be taken in order to prevent a more serious fault.

Alarm Customization

From the Alarm Customization screen you can edit each alarm by clicking on alarm from the action list.

1. From the **Diagnostics** menu, select **Customization** under the **Alarms** section.

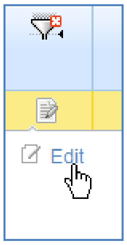


Alarm Customization

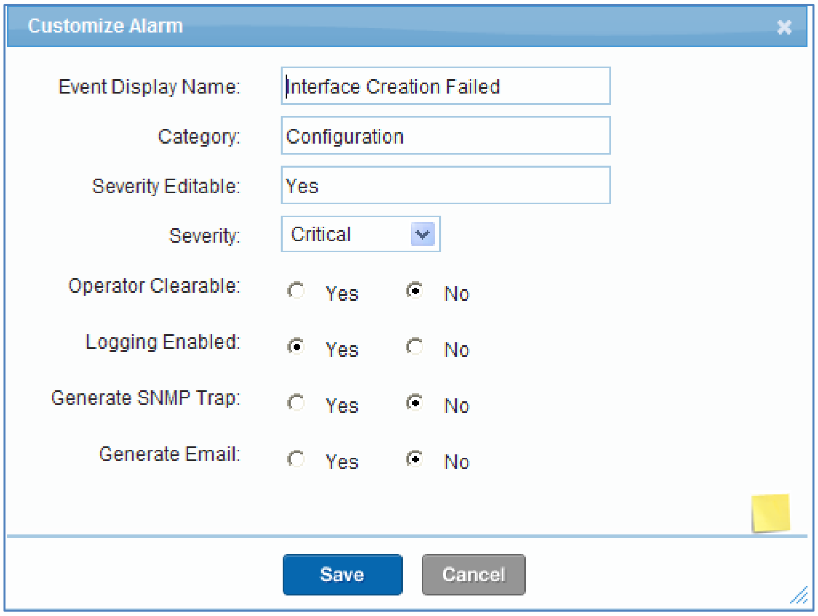
	Severity	Category	Name	Severity Editable	Operator Clearable	Logging Enabled	SNMP Traps	Email
📝	🔴	Configuration	Interface Creation Failed	Yes	No	Yes	No	No
📝	🔴	Overload	Bandwidth Limit Reached at Interface	Yes	No	Yes	Yes	Yes
📝	🟡	Security	TLS Connectivity to Un-Configured Peer Fa	Yes	No	Yes	No	No
📝	🟡	Security	TLS Connectivity to Configured Peer Failec	Yes	No	Yes	No	No
📝	🔴	Overload	Session License Limit Reached	Yes	No	Yes	No	Yes
📝	🔴	Overload	System Session Limit Reached	Yes	No	Yes	No	Yes
📝	🟠	Overload	Approaching Session License Limit	Yes	No	Yes	No	Yes
📝	🟠	Overload	Approaching System Session Limit	Yes	No	Yes	No	Yes
📝	🟠	Session	Connectivity Failure with Peer	Yes	No	Yes	No	No
📝	🔴	Configuration	Interface Activation Failed	Yes	No	Yes	No	No
📝	🔴	Configuration	Registration with Gatekeeper failed	Yes	No	Yes	No	No
📝	🟡	QoS	Packet Rate Limit exceeded at Peer	Yes	No	Yes	No	No
📝	🟡	QoS	Packet Rate Limit exceeded at Interface	Yes	No	Yes	No	No
📝	🟡	Security	Excessive Packet Drops	Yes	No	Yes	No	No
📝	🟠	Security	Peer Backlisted	Yes	No	Yes	No	No
📝	🟠	QoS	Maximum Active Sessions reached on Pee	Yes	No	Yes	No	No
📝	🟠	QoS	Maximum Active Sessions reached on Inte	Yes	No	Yes	No	No
📝	🟠	QoS	Maximum Outgoing Active Sessions reach	Yes	No	Yes	No	No
📝	🟠	QoS	Maximum Outgoing Active Sessions reach	Yes	No	Yes	No	No
📝	🟠	QoS	Maximum Incoming Active Sessions reach	Yes	No	Yes	No	No

Page 1 of 2 20 View 1 - 20 of 39

2. Click the edit button for an alarm that you want to edit the definition.



3. The following screen appears:



Event Display Name: Interface Creation Failed

Category: Configuration

Severity Editable: Yes

Severity: Critical

Operator Clearable: ○ Yes ● No

Logging Enabled: ● Yes ○ No

Generate SNMP Trap: ○ Yes ● No

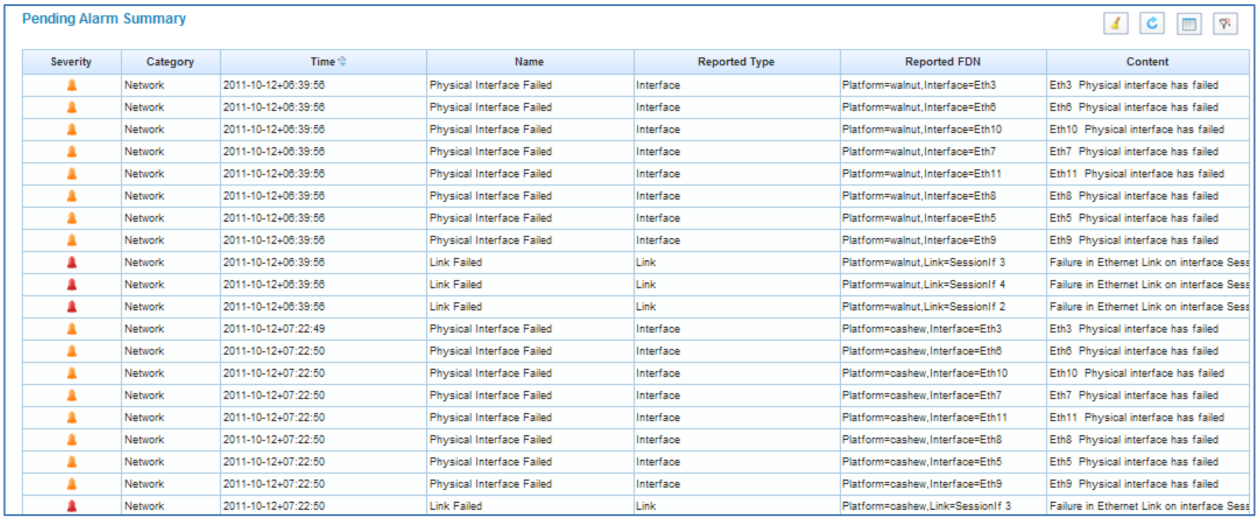
Generate Email: ○ Yes ● No

4. You can change the alarm definition including the severity.

Reporting Pending Alarms

Pending alarms are outstanding alarms that are currently reported on the BorderNet 4000 SBC that have not been cleared. Alarm history shows cleared alarms. Follow the steps below to report the pending alarms:

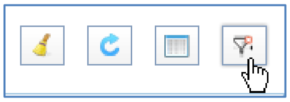
1. From the **Diagnostics** menu, select **Pending** under the **Alarms** section.



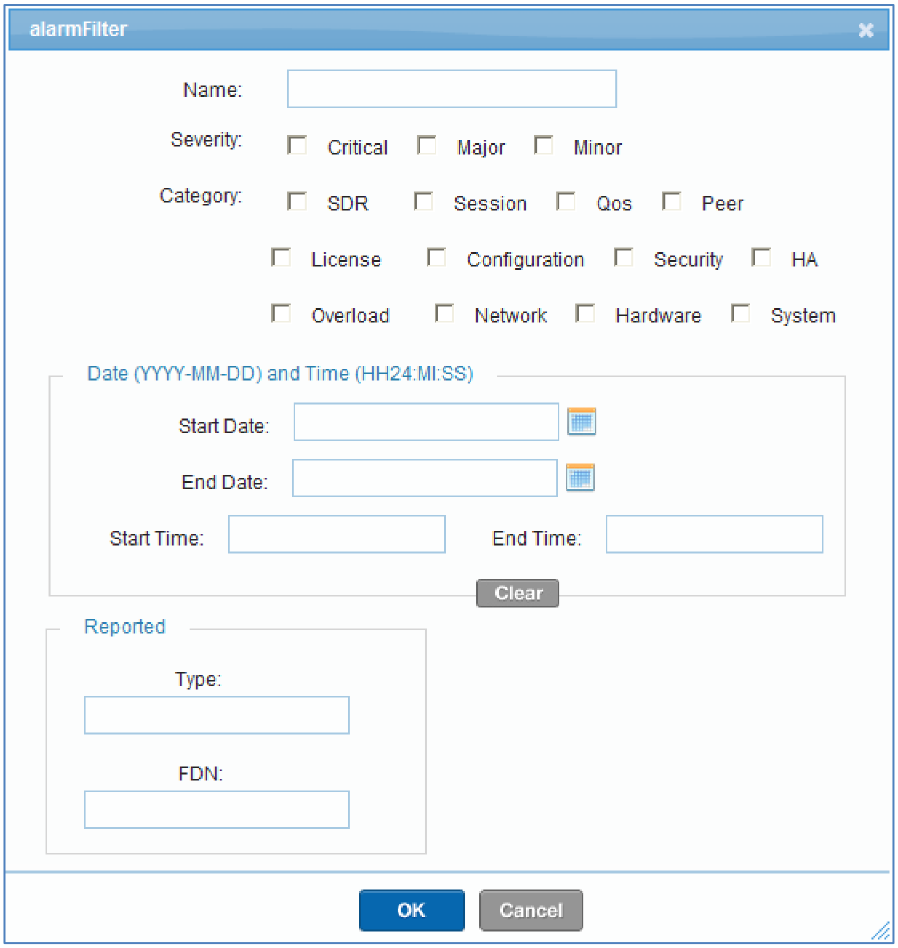
Pending Alarm Summary

Severity	Category	Time	Name	Reported Type	Reported FDN	Content
🟠	Network	2011-10-12+06:39:56	Physical Interface Failed	Interface	Platform=walnut,Interface=Eth3	Eth3 Physical interface has failed
🟠	Network	2011-10-12+06:39:56	Physical Interface Failed	Interface	Platform=walnut,Interface=Eth6	Eth6 Physical interface has failed
🟠	Network	2011-10-12+06:39:56	Physical Interface Failed	Interface	Platform=walnut,Interface=Eth10	Eth10 Physical interface has failed
🟠	Network	2011-10-12+06:39:56	Physical Interface Failed	Interface	Platform=walnut,Interface=Eth7	Eth7 Physical interface has failed
🟠	Network	2011-10-12+06:39:56	Physical Interface Failed	Interface	Platform=walnut,Interface=Eth11	Eth11 Physical interface has failed
🟠	Network	2011-10-12+06:39:56	Physical Interface Failed	Interface	Platform=walnut,Interface=Eth8	Eth8 Physical interface has failed
🟠	Network	2011-10-12+06:39:56	Physical Interface Failed	Interface	Platform=walnut,Interface=Eth5	Eth5 Physical interface has failed
🟠	Network	2011-10-12+06:39:56	Physical Interface Failed	Interface	Platform=walnut,Interface=Eth9	Eth9 Physical interface has failed
🔴	Network	2011-10-12+06:39:56	Link Failed	Link	Platform=walnut,Link=SessionIf 3	Failure in Ethernet Link on interface Sess
🔴	Network	2011-10-12+06:39:56	Link Failed	Link	Platform=walnut,Link=SessionIf 4	Failure in Ethernet Link on interface Sess
🔴	Network	2011-10-12+06:39:56	Link Failed	Link	Platform=walnut,Link=SessionIf 2	Failure in Ethernet Link on interface Sess
🟠	Network	2011-10-12+07:22:49	Physical Interface Failed	Interface	Platform=cashew,Interface=Eth3	Eth3 Physical interface has failed
🟠	Network	2011-10-12+07:22:50	Physical Interface Failed	Interface	Platform=cashew,Interface=Eth6	Eth6 Physical interface has failed
🟠	Network	2011-10-12+07:22:50	Physical Interface Failed	Interface	Platform=cashew,Interface=Eth10	Eth10 Physical interface has failed
🟠	Network	2011-10-12+07:22:50	Physical Interface Failed	Interface	Platform=cashew,Interface=Eth7	Eth7 Physical interface has failed
🟠	Network	2011-10-12+07:22:50	Physical Interface Failed	Interface	Platform=cashew,Interface=Eth11	Eth11 Physical interface has failed
🟠	Network	2011-10-12+07:22:50	Physical Interface Failed	Interface	Platform=cashew,Interface=Eth8	Eth8 Physical interface has failed
🟠	Network	2011-10-12+07:22:50	Physical Interface Failed	Interface	Platform=cashew,Interface=Eth5	Eth5 Physical interface has failed
🟠	Network	2011-10-12+07:22:50	Physical Interface Failed	Interface	Platform=cashew,Interface=Eth9	Eth9 Physical interface has failed
🔴	Network	2011-10-12+07:22:50	Link Failed	Link	Platform=cashew,Link=SessionIf 3	Failure in Ethernet Link on interface Sess

2. Click the filter button to further refine the results.



3. Change the reporting criteria from the screen below:

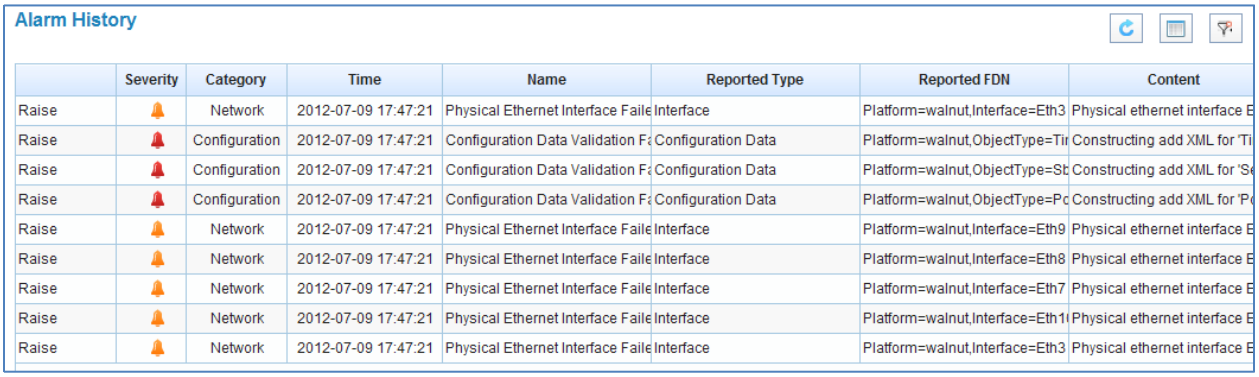

alarmFilter
Name:
Severity:
□ Critical □ Major □ Minor
Category:
□ SDR □ Session □ Qos □ Peer
□ License □ Configuration □ Security □ HA
□ Overload □ Network □ Hardware □ System
Date (YYYY-MM-DD) and Time (HH24:MI:SS)
Start Date:
End Date:
Start Time:
End Time:
Clear
Reported
Type:
FDN:
OK
Cancel

4. Select **All** in the **Show** field.
5. You can change the severity or category of the alarm.
6. Click **OK**.

Reporting Alarm History

Follow the steps below to report the history of alarms on the BorderNet 4000 SBC:

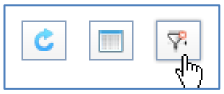
1. From the **Diagnostics** menu, select **History** under the **Alarms** section.



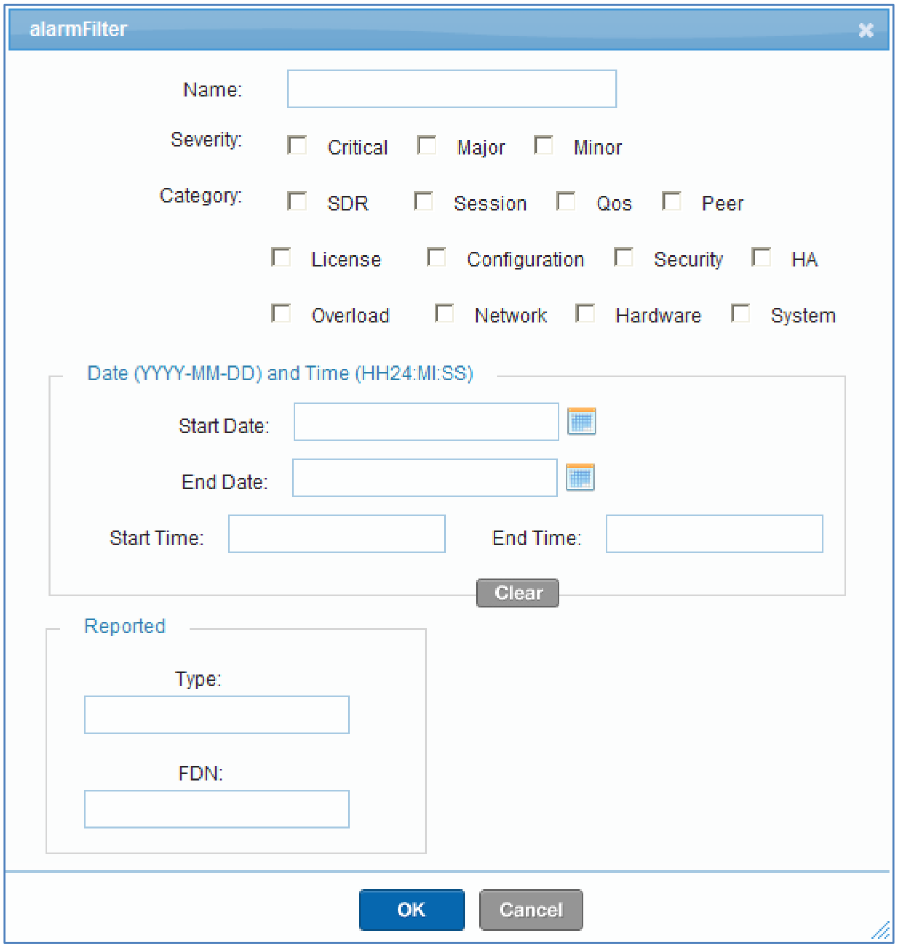
Alarm History

	Severity	Category	Time	Name	Reported Type	Reported FDN	Content
Raise	🔔	Network	2012-07-09 17:47:21	Physical Ethernet Interface Faile	Interface	Platform=walnut,Interface=Eth3	Physical ethernet interface E
Raise	🔔	Configuration	2012-07-09 17:47:21	Configuration Data Validation Fa	Configuration Data	Platform=walnut,ObjectType=Ti	Constructing add XML for 'Ti
Raise	🔔	Configuration	2012-07-09 17:47:21	Configuration Data Validation Fa	Configuration Data	Platform=walnut,ObjectType=Sb	Constructing add XML for 'Se
Raise	🔔	Configuration	2012-07-09 17:47:21	Configuration Data Validation Fa	Configuration Data	Platform=walnut,ObjectType=Pc	Constructing add XML for 'Pc
Raise	🔔	Network	2012-07-09 17:47:21	Physical Ethernet Interface Faile	Interface	Platform=walnut,Interface=Eth9	Physical ethernet interface E
Raise	🔔	Network	2012-07-09 17:47:21	Physical Ethernet Interface Faile	Interface	Platform=walnut,Interface=Eth8	Physical ethernet interface E
Raise	🔔	Network	2012-07-09 17:47:21	Physical Ethernet Interface Faile	Interface	Platform=walnut,Interface=Eth7	Physical ethernet interface E
Raise	🔔	Network	2012-07-09 17:47:21	Physical Ethernet Interface Faile	Interface	Platform=walnut,Interface=Eth1(	Physical ethernet interface E
Raise	🔔	Network	2012-07-09 17:47:21	Physical Ethernet Interface Faile	Interface	Platform=walnut,Interface=Eth3	Physical ethernet interface E

2. Click the filter button to further refine the results.



3. Change the reporting criteria from the screen below:



alarmFilter

Name:

Severity: □ Critical □ Major □ Minor

Category: □ SDR □ Session □ Qos □ Peer
□ License □ Configuration □ Security □ HA
□ Overload □ Network □ Hardware □ System

Date (YYYY-MM-DD) and Time (HH24:MI:SS)

Start Date:

End Date:

Start Time: End Time:

Reported

Type:

FDN:

See also the Alarms section in the Troubleshooting chapter.

Statistical Reports

The BorderNet 4000 SBC generates reports to show traffic and operational information. Statistical data is stored locally on the BorderNet 4000 SBC for up to seven days. Statistical data is automatically calculated at well-defined time intervals throughout the day.

To generate and view a report, you can define the time intervals to be either five minute intervals or one hour intervals for the BorderNet 4000 SBC activity. You can export the reports to Adobe PDF, Microsoft Word, or Microsoft Excel format from the WebUI.

The BorderNet 4000 automatically generates the following data:

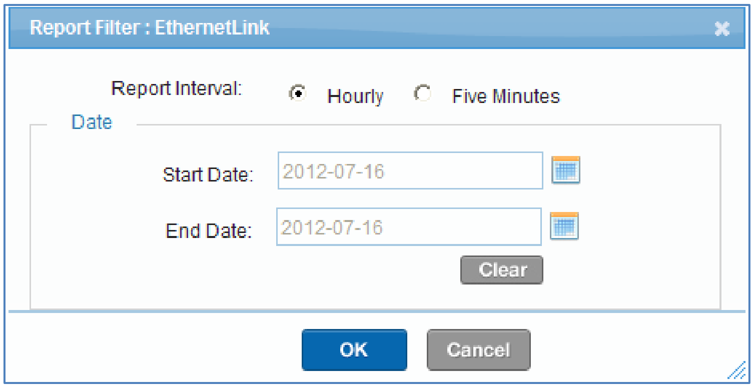
- Ethernet and CPU usage statistics
- QoS statistics, including incoming and outgoing session statistics on the following:
    - SIP and H.323 peers
    - SIP and H.323 interfaces
    - System wide
- Packet statistics, including the number of packets dropped because of various security checks.

Ethernet and CPU	• Total Receive/Transmit packets and bytes • Receive/Transmit errors	• CPU min, max and average usage
QoS	• Total Inbound Sessions • Total Inbound Sessions Rejected due to constraints violation or Insufficient Bandwidth • Highest Concurrent Inbound Sessions • Total Outbound Sessions • Total Outbound Sessions Rejected due to constraints violation or Insufficient Bandwidth	• Highest Concurrent Outbound Sessions • Peak Rate of Inbound/Outbound Traffic • Average Rate of Inbound/Outbound traffic • Total Attempts (Seizures) • Total Answered Sessions • Answer-to-Seizure Ratio Percentage
Packet Statistics	• Signaling packets received • Packets dropped by security checks	• Media packets received • Media packets dropped for different reasons

Follow the procedures in this section to run the BorderNet 4000 SBC reports.

Reporting Ethernet Links

1. From the **Diagnostics** menu, select **Ethernet Links** under **Traffic Statistics**.



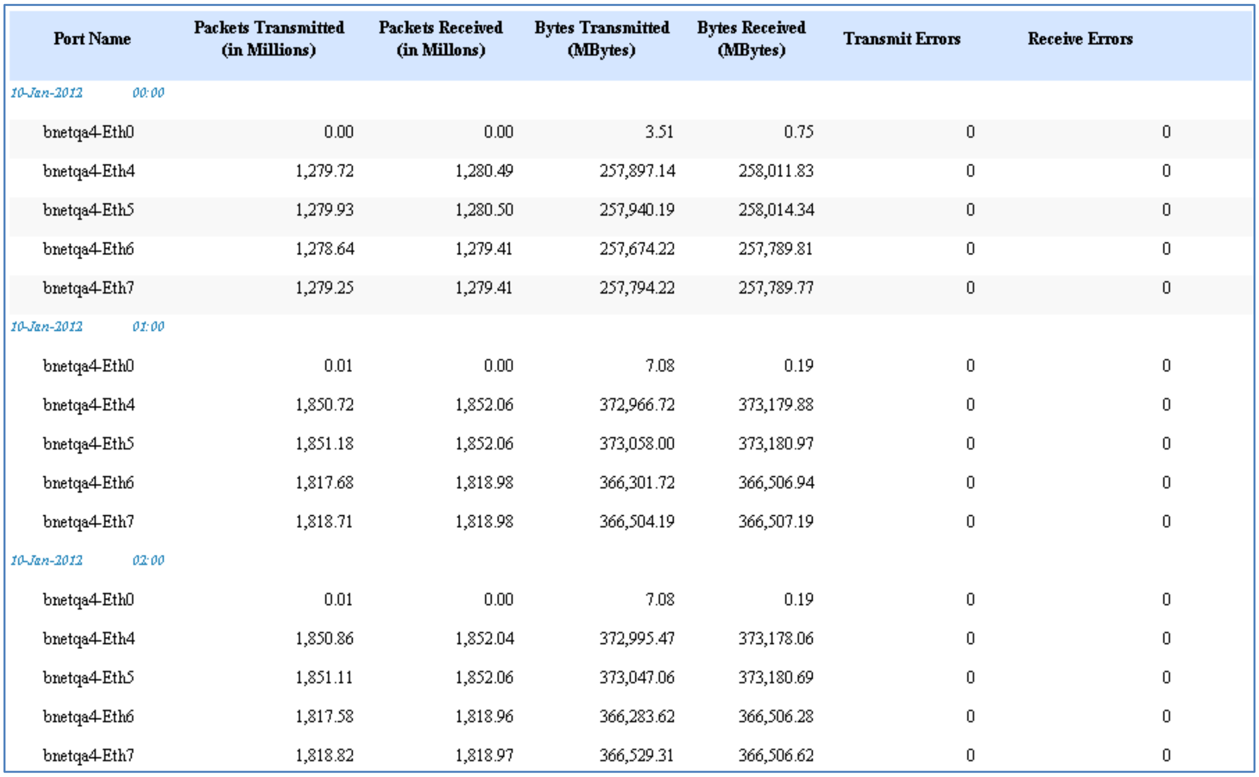
Report Interval: ● Hourly ○ Five Minutes

Date

Start Date: 2012-07-16

End Date: 2012-07-16

2. Select whether you want to report the Ethernet Links hourly or five minute intervals.
3. Select the Start Date and End Date of the period that you want to report Ethernet Links.
4. Click **OK** and the following appears.

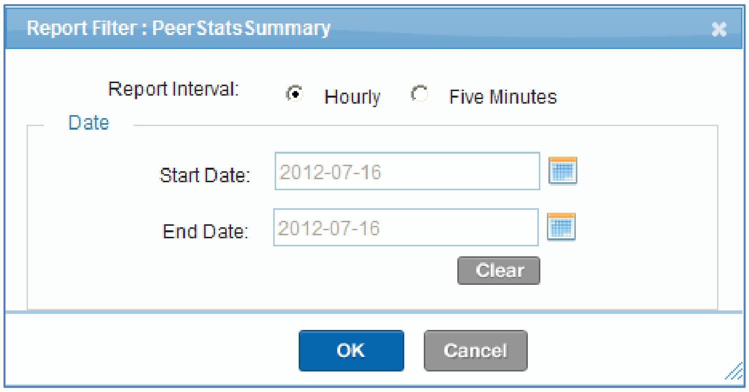


Port Name	Packets Transmitted (in Millions)	Packets Received (in Millons)	Bytes Transmitted (MBytes)	Bytes Received (MBytes)	Transmit Errors	Receive Errors
10-Jan-2012 00:00						
bnetqa4-Eth0	0.00	0.00	3.51	0.75	0	0
bnetqa4-Eth4	1,279.72	1,280.49	257,897.14	258,011.83	0	0
bnetqa4-Eth5	1,279.93	1,280.50	257,940.19	258,014.34	0	0
bnetqa4-Eth6	1,278.64	1,279.41	257,674.22	257,789.81	0	0
bnetqa4-Eth7	1,279.25	1,279.41	257,794.22	257,789.77	0	0
10-Jan-2012 01:00						
bnetqa4-Eth0	0.01	0.00	7.08	0.19	0	0
bnetqa4-Eth4	1,850.72	1,852.06	372,966.72	373,179.88	0	0
bnetqa4-Eth5	1,851.18	1,852.06	373,058.00	373,180.97	0	0
bnetqa4-Eth6	1,817.68	1,818.98	366,301.72	366,506.94	0	0
bnetqa4-Eth7	1,818.71	1,818.98	366,504.19	366,507.19	0	0
10-Jan-2012 02:00						
bnetqa4-Eth0	0.01	0.00	7.08	0.19	0	0
bnetqa4-Eth4	1,850.86	1,852.04	372,995.47	373,178.06	0	0
bnetqa4-Eth5	1,851.11	1,852.06	373,047.06	373,180.69	0	0
bnetqa4-Eth6	1,817.58	1,818.96	366,283.62	366,506.28	0	0
bnetqa4-Eth7	1,818.82	1,818.97	366,529.31	366,506.62	0	0

Peer Statistics

Reporting Summary

1. From the **Diagnostics** menu, select **Summary** under **Peer Statistics**.



Report Filter : PeerStatsSummary

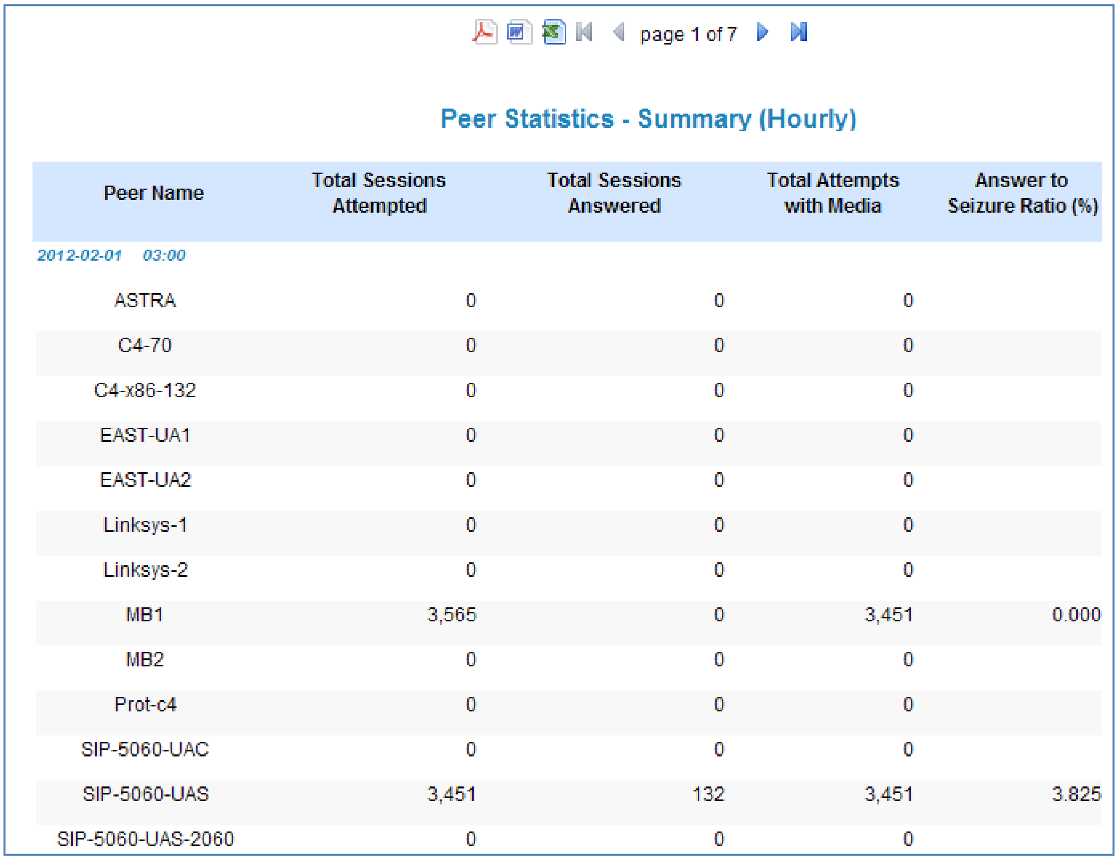
Report Interval: ● Hourly ○ Five Minutes

Date

Start Date: 2012-07-16

End Date: 2012-07-16

2. Select whether you want to report the Peer Statistics hourly or five minute intervals.
3. Select the Start Date and End Date of the period that you want to report Peer Statistics.
4. Click **OK** and the following appears.

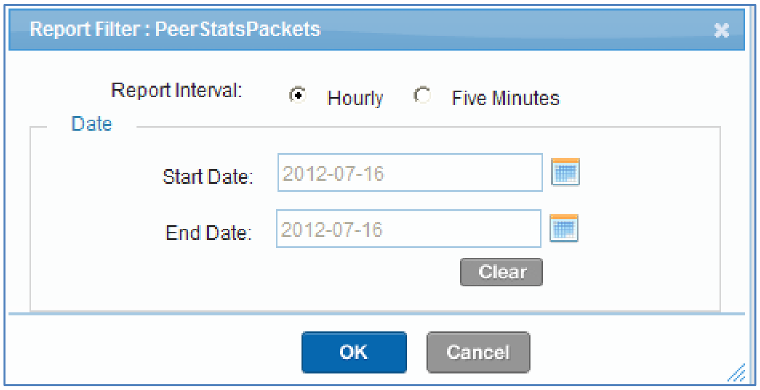


Peer Statistics - Summary (Hourly)

Peer Name	Total Sessions Attempted	Total Sessions Answered	Total Attempts with Media	Answer to Seizure Ratio (%)
2012-02-01 03:00				
ASTRA	0	0	0	
C4-70	0	0	0	
C4-x86-132	0	0	0	
EAST-UA1	0	0	0	
EAST-UA2	0	0	0	
Linksys-1	0	0	0	
Linksys-2	0	0	0	
MB1	3,565	0	3,451	0.000
MB2	0	0	0	
Prot-c4	0	0	0	
SIP-5060-UAC	0	0	0	
SIP-5060-UAS	3,451	132	3,451	3.825
SIP-5060-UAS-2060	0	0	0	

Reporting Peer Packet Statistics

1. From the **Diagnostics** menu, select **Packet Statistics** under **Peer Statistics**.



Report Filter : PeerStatsPackets

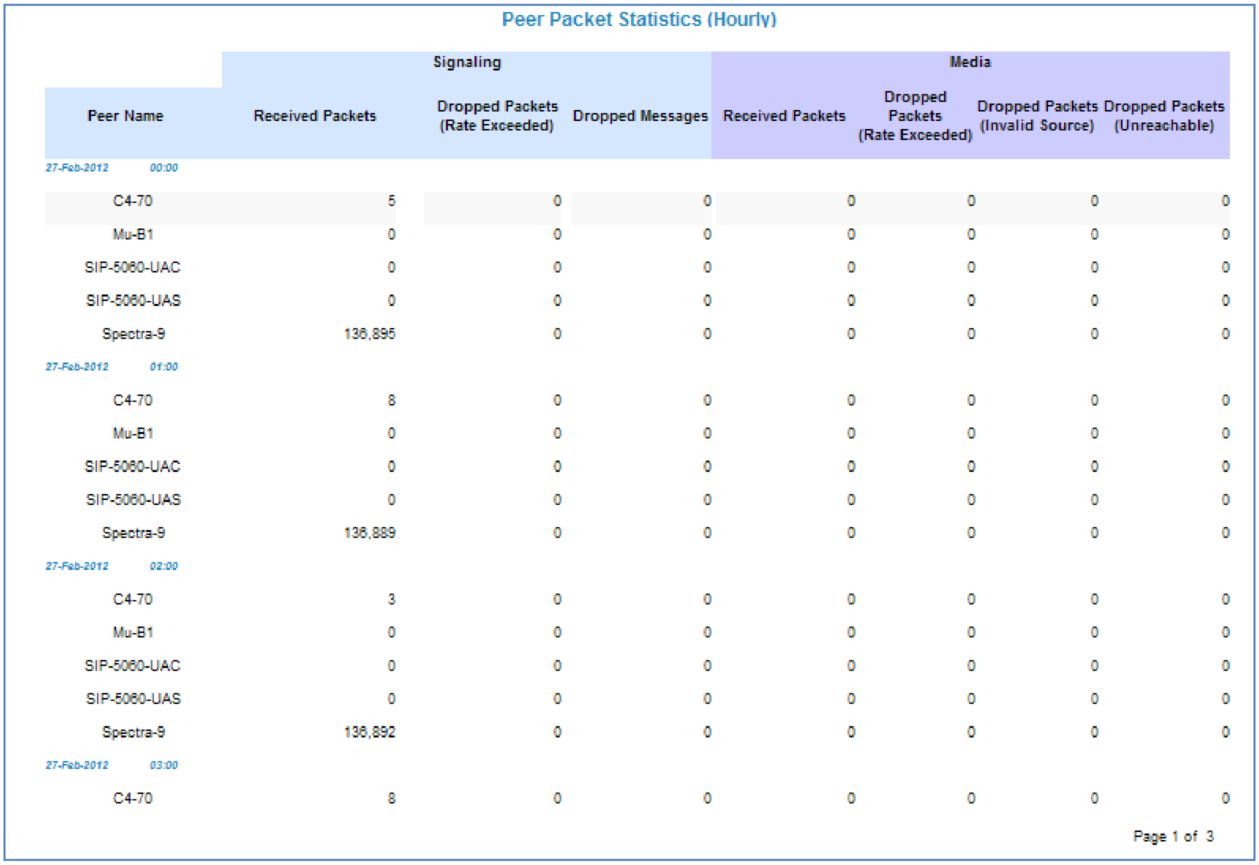
Report Interval: ● Hourly ○ Five Minutes

Date

Start Date: 2012-07-16

End Date: 2012-07-16

2. Select whether you want to report the Peer Statistics hourly (Yes) or in five minute intervals (No).
3. Select the Start Date and End Date of the period that you want to report Peer Statistics.
4. Click **OK** and the following appears:



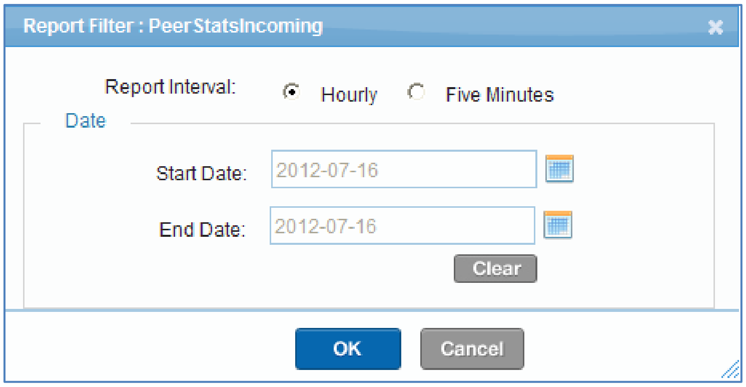
Peer Packet Statistics (Hourly)

	Signaling			Media			
Peer Name	Received Packets	Dropped Packets (Rate Exceeded)	Dropped Messages	Received Packets	Dropped Packets (Rate Exceeded)	Dropped Packets (Invalid Source)	Dropped Packets (Unreachable)
27-Feb-2012 00:00							
C4-70	5	0	0	0	0	0	0
Mu-B1	0	0	0	0	0	0	0
SIP-5060-UAC	0	0	0	0	0	0	0
SIP-5060-UAS	0	0	0	0	0	0	0
Spectra-9	136,895	0	0	0	0	0	0
27-Feb-2012 01:00							
C4-70	8	0	0	0	0	0	0
Mu-B1	0	0	0	0	0	0	0
SIP-5060-UAC	0	0	0	0	0	0	0
SIP-5060-UAS	0	0	0	0	0	0	0
Spectra-9	136,889	0	0	0	0	0	0
27-Feb-2012 02:00							
C4-70	3	0	0	0	0	0	0
Mu-B1	0	0	0	0	0	0	0
SIP-5060-UAC	0	0	0	0	0	0	0
SIP-5060-UAS	0	0	0	0	0	0	0
Spectra-9	136,892	0	0	0	0	0	0
27-Feb-2012 03:00							
C4-70	8	0	0	0	0	0	0

Page 1 of 3

Reporting Incoming Sessions

1. From the **Diagnostics** menu, select **Incoming Session** under **Peer Statistics**.



Report Filter : PeerStatsIncoming

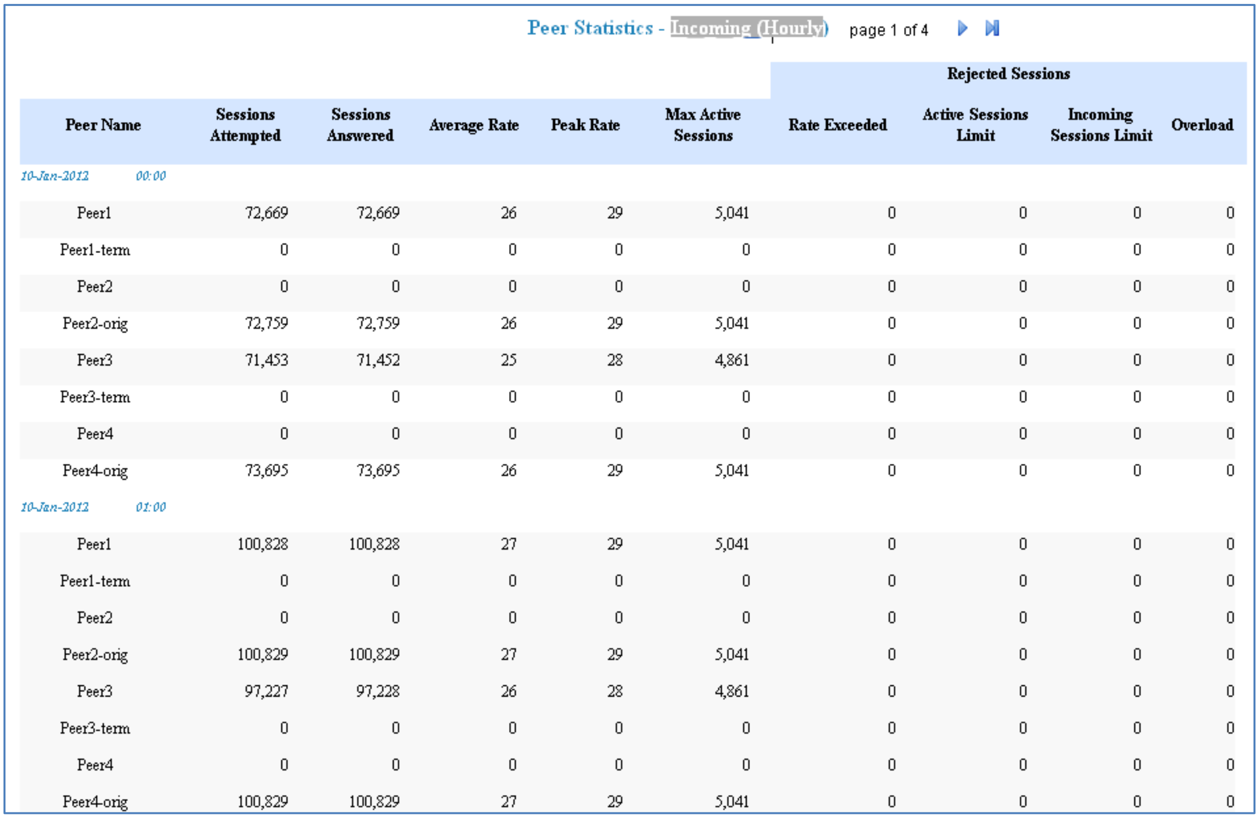
Report Interval: ● Hourly ○ Five Minutes

Date

Start Date: 2012-07-16

End Date: 2012-07-16

2. Select whether you want to report the Peer Statistics hourly or five minute intervals.
3. Select the Start Date and End Date of the period that you want to report Peer Statistics.
4. Click **OK** and the following screen appears.

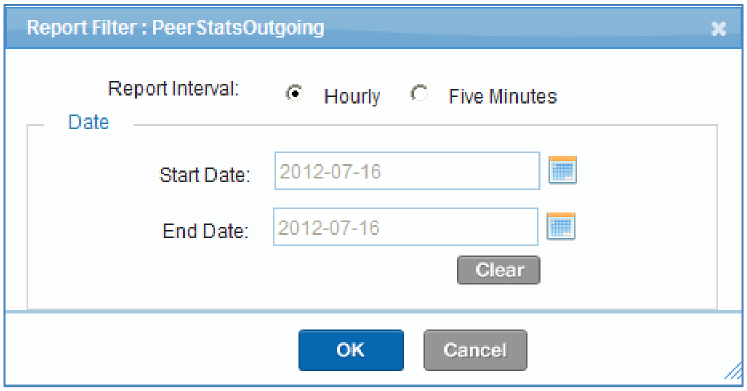


Peer Statistics - Incoming (Hourly) page 1 of 4

						Rejected Sessions			
Peer Name	Sessions Attempted	Sessions Answered	Average Rate	Peak Rate	Max Active Sessions	Rate Exceeded	Active Sessions Limit	Incoming Sessions Limit	Overload
10-Jan-2012 00:00									
Peer1	72,669	72,669	26	29	5,041	0	0	0	0
Peer1-term	0	0	0	0	0	0	0	0	0
Peer2	0	0	0	0	0	0	0	0	0
Peer2-orig	72,759	72,759	26	29	5,041	0	0	0	0
Peer3	71,453	71,452	25	28	4,861	0	0	0	0
Peer3-term	0	0	0	0	0	0	0	0	0
Peer4	0	0	0	0	0	0	0	0	0
Peer4-orig	73,695	73,695	26	29	5,041	0	0	0	0
10-Jan-2012 01:00									
Peer1	100,828	100,828	27	29	5,041	0	0	0	0
Peer1-term	0	0	0	0	0	0	0	0	0
Peer2	0	0	0	0	0	0	0	0	0
Peer2-orig	100,829	100,829	27	29	5,041	0	0	0	0
Peer3	97,227	97,228	26	28	4,861	0	0	0	0
Peer3-term	0	0	0	0	0	0	0	0	0
Peer4	0	0	0	0	0	0	0	0	0
Peer4-orig	100,829	100,829	27	29	5,041	0	0	0	0

Reporting Outgoing Sessions

1. From the **Diagnostics** menu, select **Outgoing Sessions** under **Peer Statistics**.



Report Filter : PeerStatsOutgoing

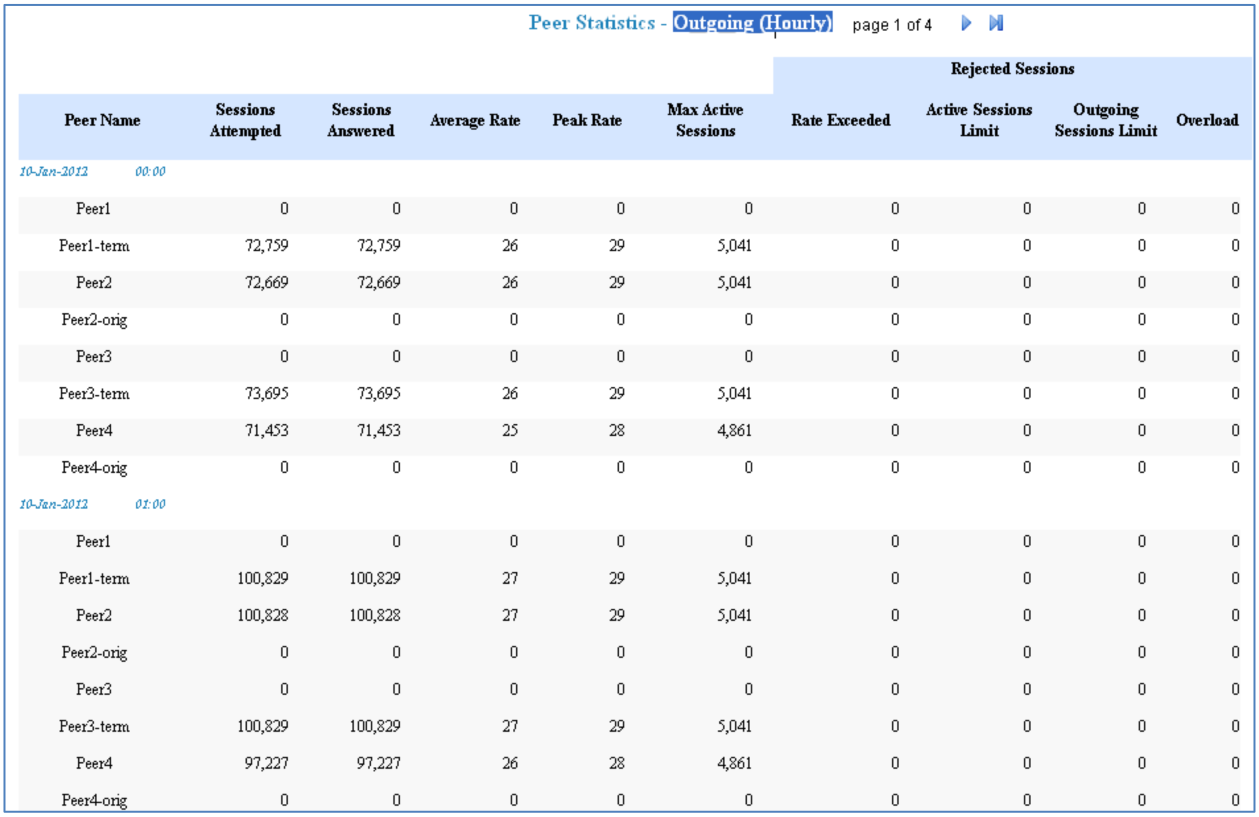
Report Interval: ● Hourly ○ Five Minutes

Date

Start Date: 2012-07-16

End Date: 2012-07-16

2. Select whether you want to report the Peer Statistics hourly or five minute intervals.
3. Select the Start Date and End Date of the period that you want to report Peer Statistics.
4. Click **OK** and the following appears.



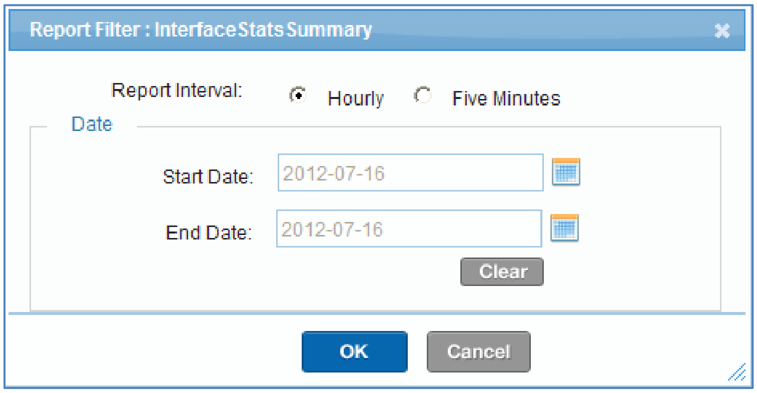
Peer Statistics - Outgoing (Hourly) page 1 of 4

						Rejected Sessions			
Peer Name	Sessions Attempted	Sessions Answered	Average Rate	Peak Rate	Max Active Sessions	Rate Exceeded	Active Sessions Limit	Outgoing Sessions Limit	Overload
10-Jan-2012 00:00									
Peer1	0	0	0	0	0	0	0	0	0
Peer1-term	72,759	72,759	26	29	5,041	0	0	0	0
Peer2	72,669	72,669	26	29	5,041	0	0	0	0
Peer2-orig	0	0	0	0	0	0	0	0	0
Peer3	0	0	0	0	0	0	0	0	0
Peer3-term	73,695	73,695	26	29	5,041	0	0	0	0
Peer4	71,453	71,453	25	28	4,861	0	0	0	0
Peer4-orig	0	0	0	0	0	0	0	0	0
10-Jan-2012 01:00									
Peer1	0	0	0	0	0	0	0	0	0
Peer1-term	100,829	100,829	27	29	5,041	0	0	0	0
Peer2	100,828	100,828	27	29	5,041	0	0	0	0
Peer2-orig	0	0	0	0	0	0	0	0	0
Peer3	0	0	0	0	0	0	0	0	0
Peer3-term	100,829	100,829	27	29	5,041	0	0	0	0
Peer4	97,227	97,227	26	28	4,861	0	0	0	0
Peer4-orig	0	0	0	0	0	0	0	0	0

Interface Statistics

Reporting Summary

1. From the **Diagnostics** menu, select **Summary** under **Interface Statistics**.

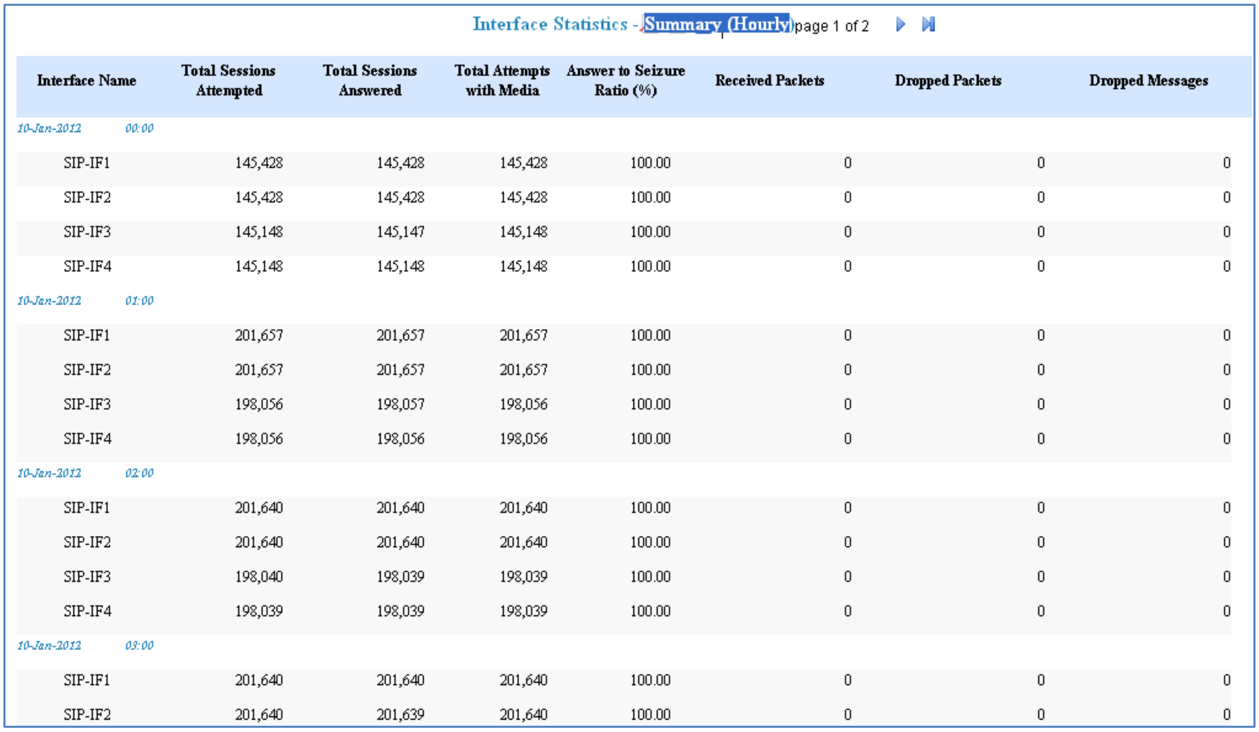


Report Interval: ● Hourly ○ Five Minutes

Start Date: 2012-07-16

End Date: 2012-07-16

2. Select whether you want to report the Interface Statistics hourly or five minute intervals.
3. Select the Start Date and End Date of the period that you want to report Interface Statistics.
4. Click **OK** and the following appears.

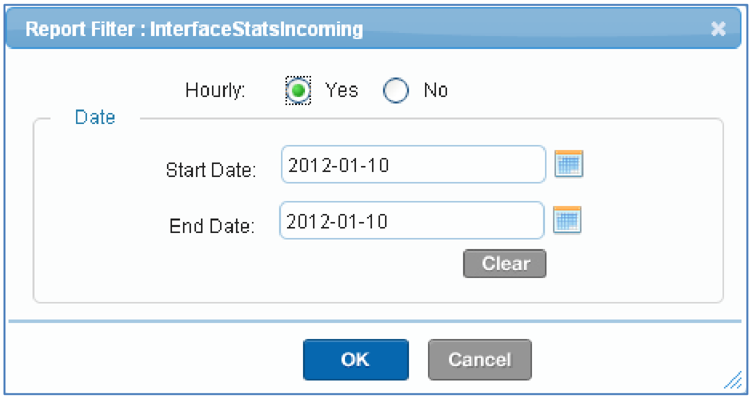


Interface Statistics - Summary (Hourly) page 1 of 2

Interface Name	Total Sessions Attempted	Total Sessions Answered	Total Attempts with Media	Answer to Seizure Ratio (%)	Received Packets	Dropped Packets	Dropped Messages
10-Jan-2012 00:00							
SIP-IF1	145,428	145,428	145,428	100.00	0	0	0
SIP-IF2	145,428	145,428	145,428	100.00	0	0	0
SIP-IF3	145,148	145,147	145,148	100.00	0	0	0
SIP-IF4	145,148	145,148	145,148	100.00	0	0	0
10-Jan-2012 01:00							
SIP-IF1	201,657	201,657	201,657	100.00	0	0	0
SIP-IF2	201,657	201,657	201,657	100.00	0	0	0
SIP-IF3	198,056	198,057	198,056	100.00	0	0	0
SIP-IF4	198,056	198,056	198,056	100.00	0	0	0
10-Jan-2012 02:00							
SIP-IF1	201,640	201,640	201,640	100.00	0	0	0
SIP-IF2	201,640	201,640	201,640	100.00	0	0	0
SIP-IF3	198,040	198,039	198,039	100.00	0	0	0
SIP-IF4	198,039	198,039	198,039	100.00	0	0	0
10-Jan-2012 03:00							
SIP-IF1	201,640	201,640	201,640	100.00	0	0	0
SIP-IF2	201,640	201,639	201,640	100.00	0	0	0

Reporting Incoming Sessions

1. From the **Diagnostics** menu, select **Incoming Sessions** under **Interface Statistics**.



Report Filter : InterfaceStatsIncoming

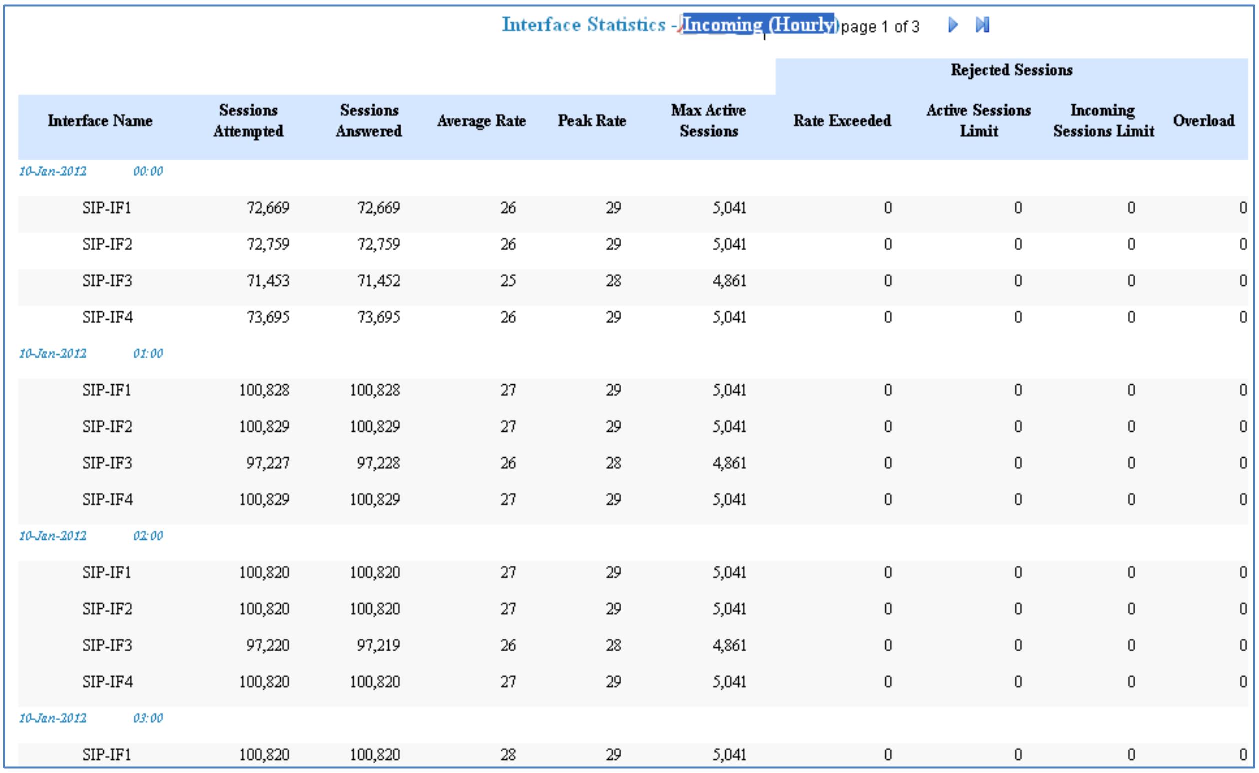
Hourly: ● Yes ○ No

Date

Start Date: 2012-01-10

End Date: 2012-01-10

2. Select whether you want to report the Interface Statistics hourly or five minute intervals.
3. Select the Start Date and End Date of the period that you want to report Interface Statistics.
4. Click **OK** and the following appears.

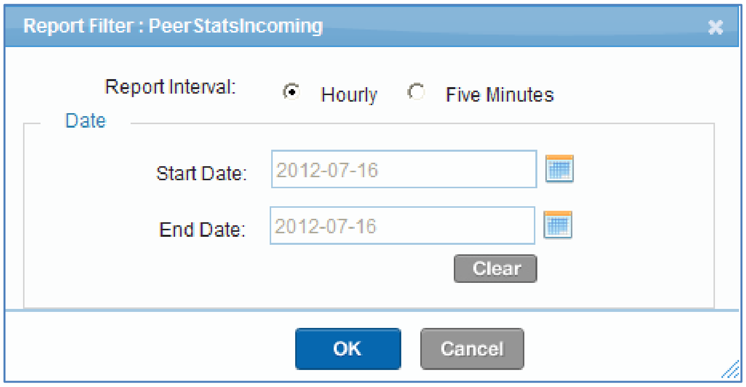


Interface Statistics - Incoming (Hourly) page 1 of 3

						Rejected Sessions			
Interface Name	Sessions Attempted	Sessions Answered	Average Rate	Peak Rate	Max Active Sessions	Rate Exceeded	Active Sessions Limit	Incoming Sessions Limit	Overload
10-Jan-2012 00:00									
SIP-IF1	72,669	72,669	26	29	5,041	0	0	0	0
SIP-IF2	72,759	72,759	26	29	5,041	0	0	0	0
SIP-IF3	71,453	71,452	25	28	4,861	0	0	0	0
SIP-IF4	73,695	73,695	26	29	5,041	0	0	0	0
10-Jan-2012 01:00									
SIP-IF1	100,828	100,828	27	29	5,041	0	0	0	0
SIP-IF2	100,829	100,829	27	29	5,041	0	0	0	0
SIP-IF3	97,227	97,228	26	28	4,861	0	0	0	0
SIP-IF4	100,829	100,829	27	29	5,041	0	0	0	0
10-Jan-2012 02:00									
SIP-IF1	100,820	100,820	27	29	5,041	0	0	0	0
SIP-IF2	100,820	100,820	27	29	5,041	0	0	0	0
SIP-IF3	97,220	97,219	26	28	4,861	0	0	0	0
SIP-IF4	100,820	100,820	27	29	5,041	0	0	0	0
10-Jan-2012 03:00									
SIP-IF1	100,820	100,820	28	29	5,041	0	0	0	0

Reporting Outgoing Sessions

1. From the **Diagnostics** menu, select **Outgoing Sessions** under **Interface Statistics**.

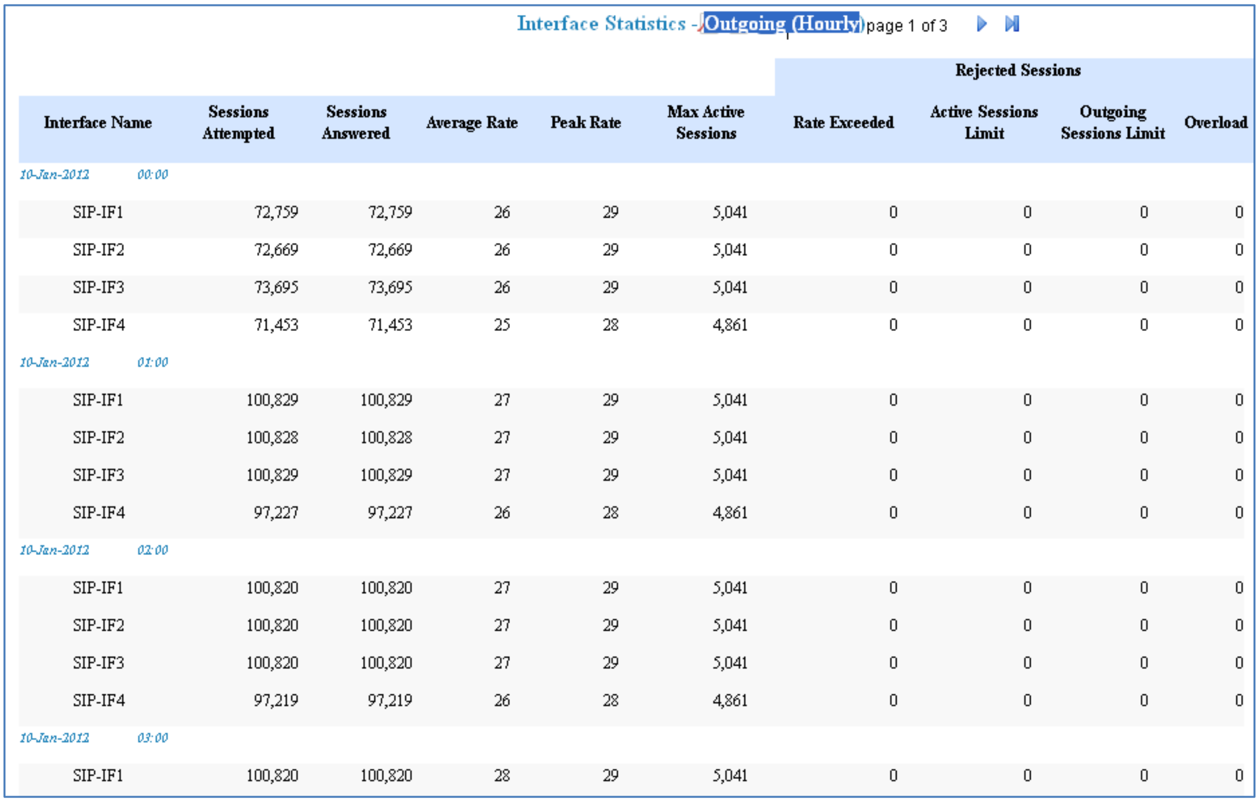


Report Interval: ● Hourly ○ Five Minutes

Start Date: 2012-07-16

End Date: 2012-07-16

2. Select whether you want to report the Interface Statistics hourly or five minute intervals.
3. Select the Start Date and End Date of the period that you want to report Interface Statistics.
4. Click **OK** and the following appears.



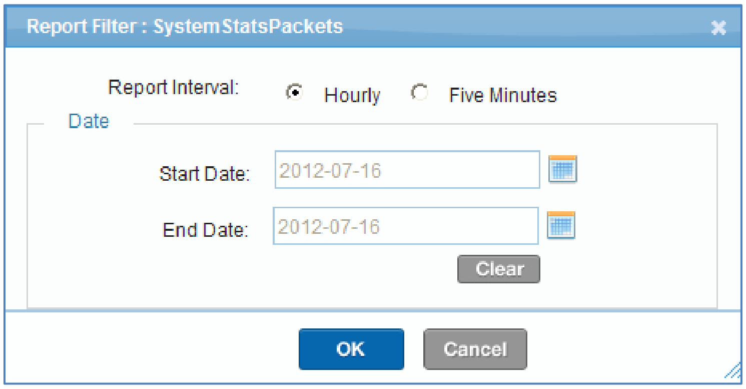
Interface Statistics - Outgoing (Hourly) page 1 of 3

						Rejected Sessions			
Interface Name	Sessions Attempted	Sessions Answered	Average Rate	Peak Rate	Max Active Sessions	Rate Exceeded	Active Sessions Limit	Outgoing Sessions Limit	Overload
10-Jan-2012 00:00									
SIP-IF1	72,759	72,759	26	29	5,041	0	0	0	0
SIP-IF2	72,669	72,669	26	29	5,041	0	0	0	0
SIP-IF3	73,695	73,695	26	29	5,041	0	0	0	0
SIP-IF4	71,453	71,453	25	28	4,861	0	0	0	0
10-Jan-2012 01:00									
SIP-IF1	100,829	100,829	27	29	5,041	0	0	0	0
SIP-IF2	100,828	100,828	27	29	5,041	0	0	0	0
SIP-IF3	100,829	100,829	27	29	5,041	0	0	0	0
SIP-IF4	97,227	97,227	26	28	4,861	0	0	0	0
10-Jan-2012 02:00									
SIP-IF1	100,820	100,820	27	29	5,041	0	0	0	0
SIP-IF2	100,820	100,820	27	29	5,041	0	0	0	0
SIP-IF3	100,820	100,820	27	29	5,041	0	0	0	0
SIP-IF4	97,219	97,219	26	28	4,861	0	0	0	0
10-Jan-2012 03:00									
SIP-IF1	100,820	100,820	28	29	5,041	0	0	0	0

System Statistics

Reporting Packet Statistics

1. From the **Diagnostics** menu, select **Packet Statistics** under **System Statistics**.



Report Filter : SystemStatsPackets

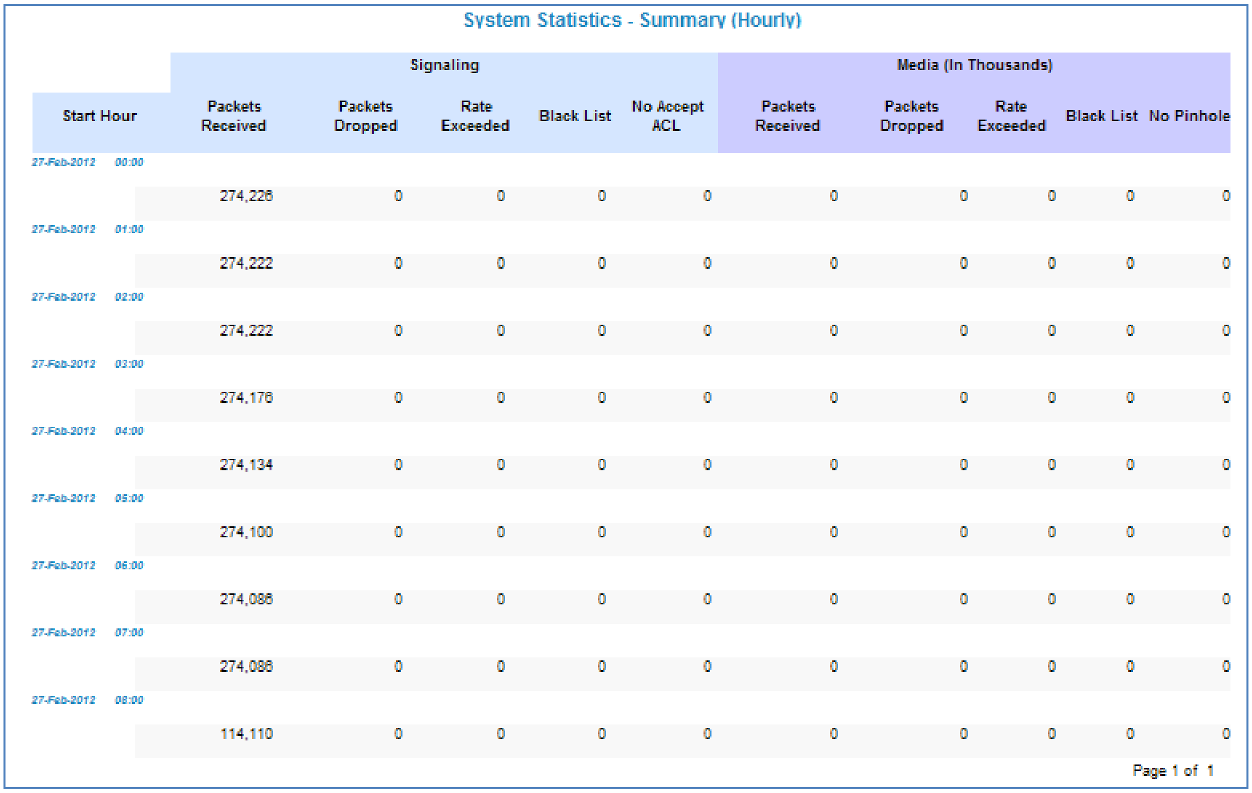
Report Interval: ● Hourly ○ Five Minutes

Date

Start Date: 2012-07-16

End Date: 2012-07-16

2. Select whether you want to report the System Statistics hourly or five minute intervals.
3. Select the Start Date and End Date of the period that you want to report System Statistics.
4. Click **OK** and the following appears.



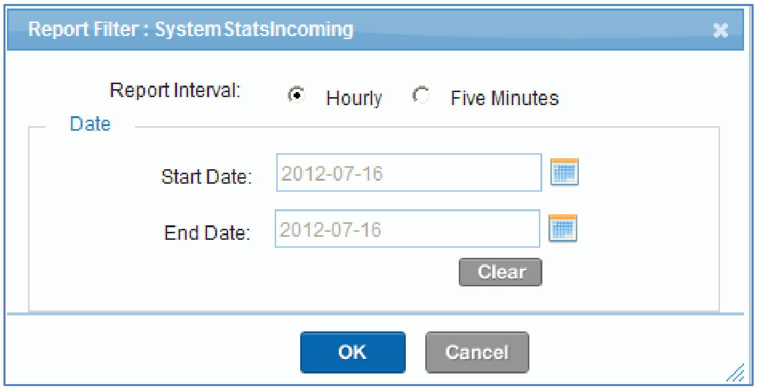
System Statistics - Summary (Hourly)

	Signaling					Media (In Thousands)				
Start Hour	Packets Received	Packets Dropped	Rate Exceeded	Black List	No Accept ACL	Packets Received	Packets Dropped	Rate Exceeded	Black List	No Pinhole
27-Feb-2012 00:00	274,226	0	0	0	0	0	0	0	0	0
27-Feb-2012 01:00	274,222	0	0	0	0	0	0	0	0	0
27-Feb-2012 02:00	274,222	0	0	0	0	0	0	0	0	0
27-Feb-2012 03:00	274,176	0	0	0	0	0	0	0	0	0
27-Feb-2012 04:00	274,134	0	0	0	0	0	0	0	0	0
27-Feb-2012 05:00	274,100	0	0	0	0	0	0	0	0	0
27-Feb-2012 06:00	274,086	0	0	0	0	0	0	0	0	0
27-Feb-2012 07:00	274,086	0	0	0	0	0	0	0	0	0
27-Feb-2012 08:00	114,110	0	0	0	0	0	0	0	0	0

Page 1 of 1

Reporting Incoming Statistics

1. From the **Diagnostics** menu, select **Incoming Sessions** under **System Statistics**.



Report Filter : SystemStatsIncoming

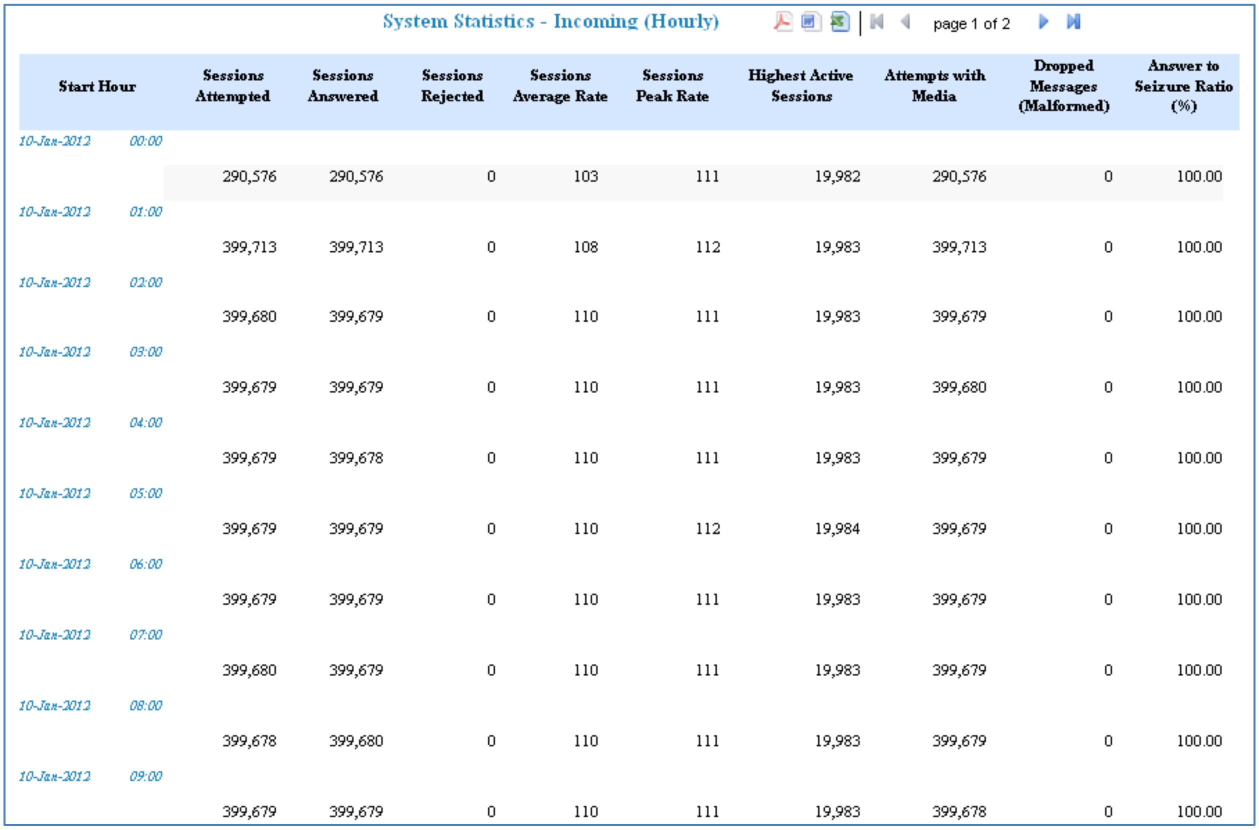
Report Interval: ● Hourly ○ Five Minutes

Date

Start Date: 2012-07-16

End Date: 2012-07-16

2. Select whether you want to report the System Statistics hourly or five minute intervals.
3. Select the Start Date and End Date of the period that you want to report System Statistics.
4. Click **OK** and the following appears.

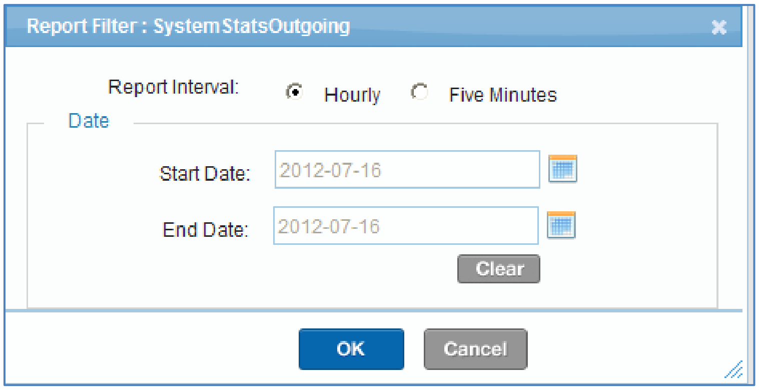


System Statistics - Incoming (Hourly)

Start Hour	Sessions Attempted	Sessions Answered	Sessions Rejected	Sessions Average Rate	Sessions Peak Rate	Highest Active Sessions	Attempts with Media	Dropped Messages (Malformed)	Answer to Seizure Ratio (%)
10-Jan-2012 00:00	290,576	290,576	0	103	111	19,982	290,576	0	100.00
10-Jan-2012 01:00	399,713	399,713	0	108	112	19,983	399,713	0	100.00
10-Jan-2012 02:00	399,680	399,679	0	110	111	19,983	399,679	0	100.00
10-Jan-2012 03:00	399,679	399,679	0	110	111	19,983	399,680	0	100.00
10-Jan-2012 04:00	399,679	399,678	0	110	111	19,983	399,679	0	100.00
10-Jan-2012 05:00	399,679	399,679	0	110	112	19,984	399,679	0	100.00
10-Jan-2012 06:00	399,679	399,679	0	110	111	19,983	399,679	0	100.00
10-Jan-2012 07:00	399,680	399,679	0	110	111	19,983	399,679	0	100.00
10-Jan-2012 08:00	399,678	399,680	0	110	111	19,983	399,679	0	100.00
10-Jan-2012 09:00	399,679	399,679	0	110	111	19,983	399,678	0	100.00

Reporting Outgoing Sessions

1. From the **Diagnostics** menu, select **Outgoing Sessions** under **System Statistics**.



Report Filter : SystemStatsOutgoing

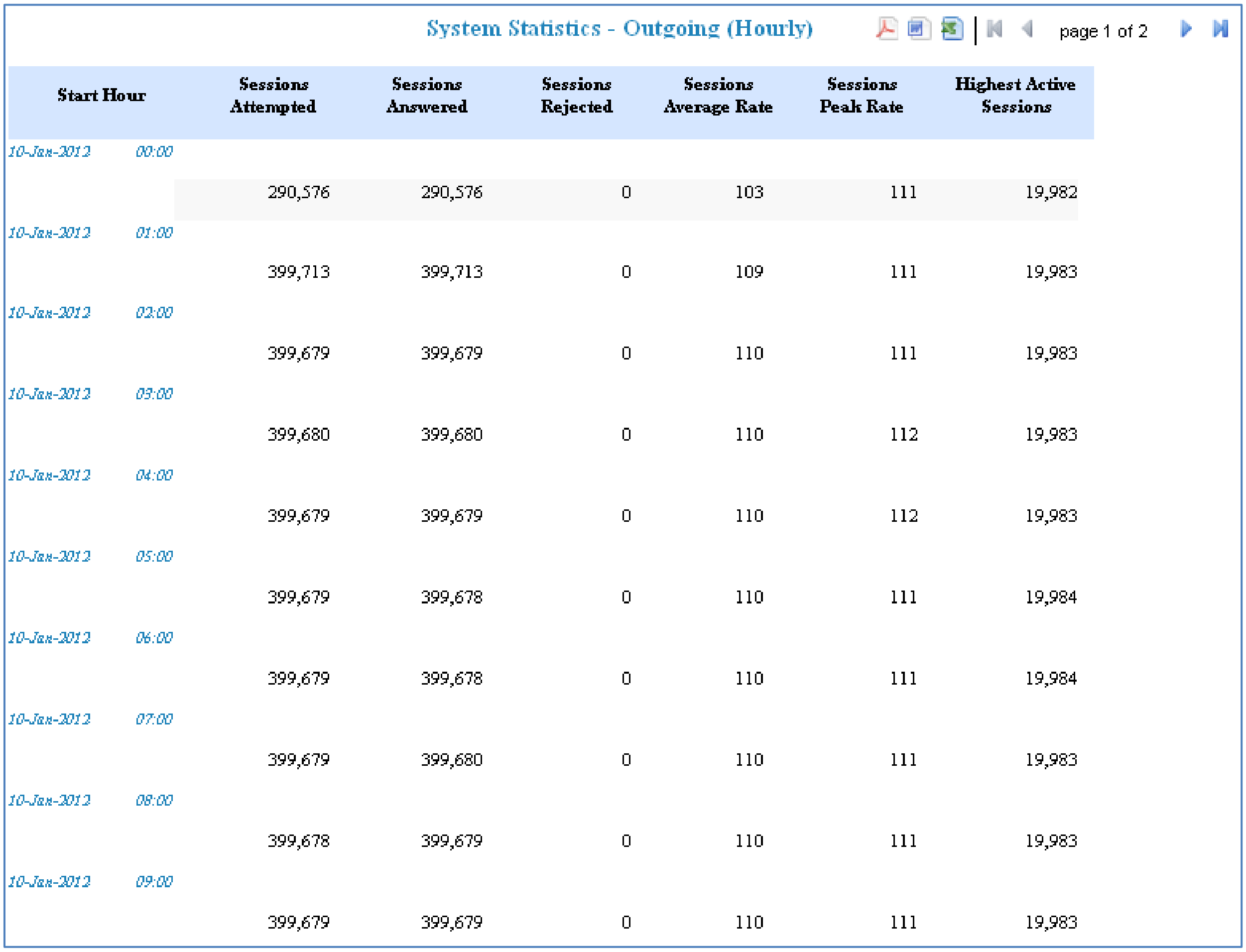
Report Interval: ● Hourly ○ Five Minutes

Date

Start Date: 2012-07-16

End Date: 2012-07-16

2. Select whether you want to report the System Statistics hourly or five minute intervals.
3. Select the Start Date and End Date of the period that you want to report System Statistics.
4. Click **OK** and the following appears.



System Statistics - Outgoing (Hourly)

Start Hour	Sessions Attempted	Sessions Answered	Sessions Rejected	Sessions Average Rate	Sessions Peak Rate	Highest Active Sessions
10-Jan-2012 00:00	290,576	290,576	0	103	111	19,982
10-Jan-2012 01:00	399,713	399,713	0	109	111	19,983
10-Jan-2012 02:00	399,679	399,679	0	110	111	19,983
10-Jan-2012 03:00	399,680	399,680	0	110	112	19,983
10-Jan-2012 04:00	399,679	399,679	0	110	112	19,983
10-Jan-2012 05:00	399,679	399,678	0	110	111	19,984
10-Jan-2012 06:00	399,679	399,678	0	110	111	19,984
10-Jan-2012 07:00	399,679	399,680	0	110	111	19,983
10-Jan-2012 08:00	399,678	399,679	0	110	111	19,983
10-Jan-2012 09:00	399,679	399,679	0	110	111	19,983

Tracing

The BorderNet 4000 SBC supports Wireshark remote tracing. The BorderNet 4000 SBC enhances the remote trace functionality of Wireshark with a custom wpcap.dll. The custom plug-in supports additional message based filters along with the existing IP level filters. All messages that match the filter are streamed to Wireshark client in pcap format.

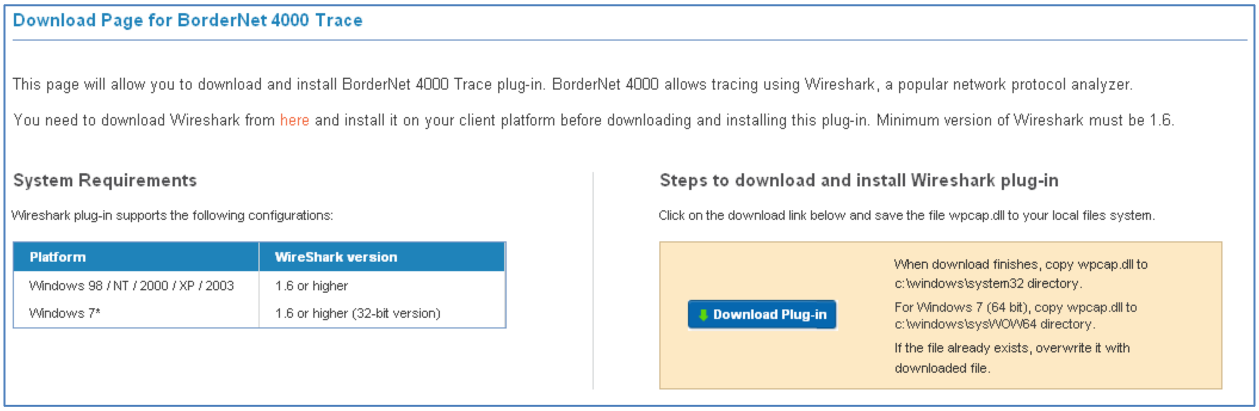
Note: The Wireshark application is not included with the BorderNet 4000 SBC. See the link on the screen below to download the application from wireshark.org. Once you have downloaded Wireshark and installed it, you can download the plug-in also from the screen below.

Wireshark uses remote tracing to capture the trace messages. You can also store the messages. By default, the BorderNet 4000 SBC streams to the Wireshark client. The custom plug-in allows profile-based traces and interface traces.

Downloading the Trace Plug-in

Follow the steps to download the Trace Plug-in:

1. From the **Diagnostics** menu, select **Plugin** under the **Trace** section.
2. Follow the instructions from screen below.



Download Page for BorderNet 4000 Trace

This page will allow you to download and install BorderNet 4000 Trace plug-in. BorderNet 4000 allows tracing using Wireshark, a popular network protocol analyzer.

You need to download Wireshark from here and install it on your client platform before downloading and installing this plug-in. Minimum version of Wireshark must be 1.6.

System Requirements

Wireshark plug-in supports the following configurations:

Platform	WireShark version
Windows 98 / NT / 2000 / XP / 2003	1.6 or higher
Windows 7*	1.6 or higher (32-bit version)

Steps to download and install Wireshark plug-in

Click on the download link below and save the file wpcap.dll to your local files system.

When download finishes, copy wpcap.dll to c:\windows\system32 directory.

For Windows 7 (64 bit), copy wpcap.dll to c:\windows\sysWOW64 directory.

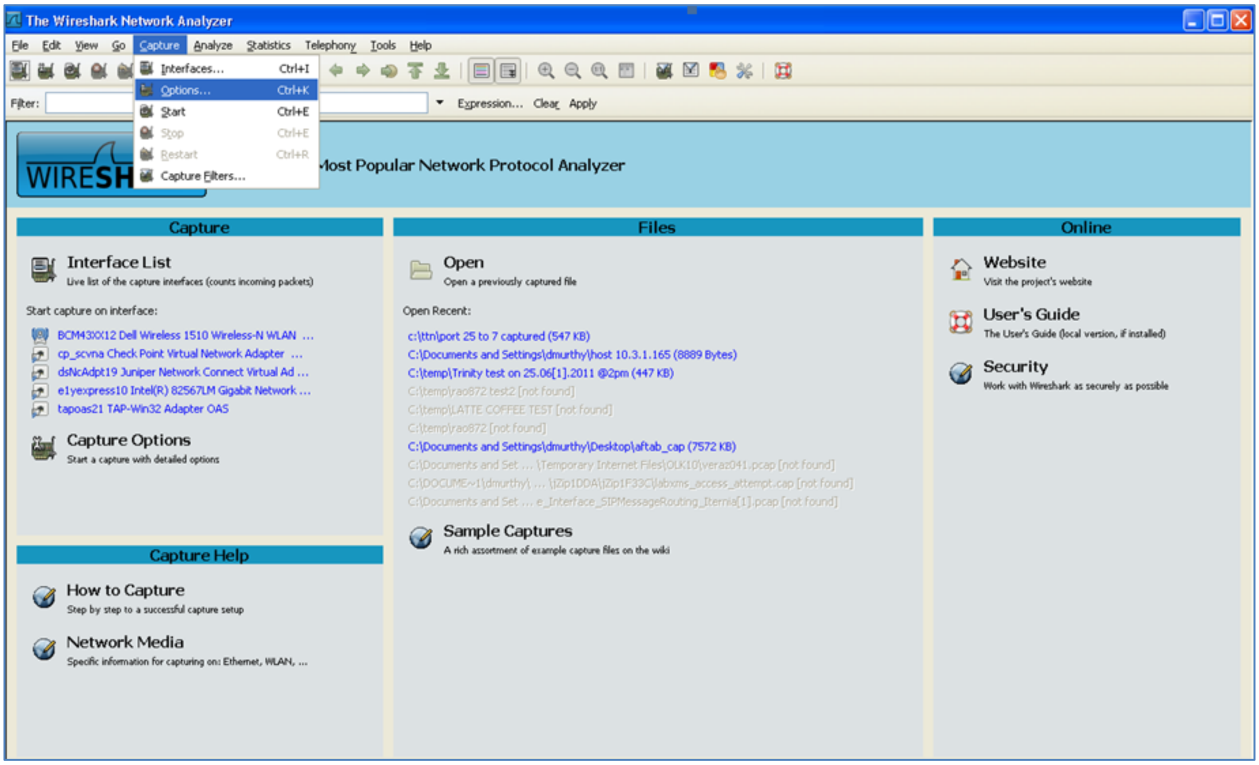
If the file already exists, overwrite it with downloaded file.

Caution: If you have previously downloaded another plug-in named wpcap.dll for a different device, do not overwrite it. Rename it before downloading this wpcap.dll.

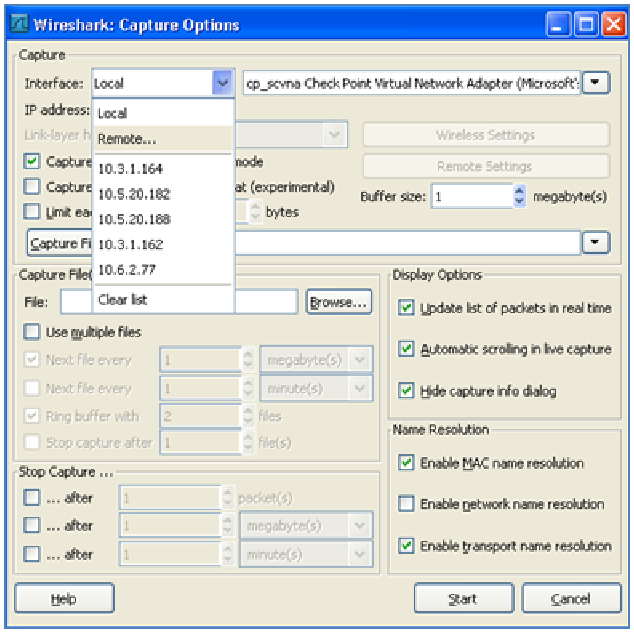
Connecting to the BorderNet 4000 SBC from Wireshark

Follow the steps below to connect to the BorderNet 4000 SBC from Wireshark:

1. Select **Options** from the **Capture** menu.


The Wireshark Network Analyzer
File Edit View Go Capture Analyze Statistics Telephony Tools Help
Interfaces... Ctrl+I
Options... Ctrl+K
Start Ctrl+E
Stop Ctrl+E
Restart Ctrl+R
Capture Filters...
Filter:
Expression... Clear Apply
WIRESH
Most Popular Network Protocol Analyzer
Capture
Interface List
Live list of the capture interfaces (counts incoming packets)
Start capture on interface:
BCM43XX12 Dell Wireless 1510 Wireless-N WLAN ...
cp_scvna Check Point Virtual Network Adapter ...
dsNcAdpt19 Juniper Network Connect Virtual Ad ...
e1yexpress10 Intel(R) 82567LM Gigabit Network ...
tapoas21 TAP-Win32 Adapter OAS
Capture Options
Start a capture with detailed options
Capture Help
How to Capture
Step by step to a successful capture setup
Network Media
Specific information for capturing on: Ethernet, WLAN, ...
Files
Open
Open a previously captured file
Open Recent:
c:\ttn\port 25 to 7 captured (547 KB)
C:\Documents and Settings\dmurthy\host 10.3.1.165 (8889 Bytes)
C:\temp\Trinity test on 25.06[1].2011 @2pm (447 KB)
C:\temp\rao872 test2 [not found]
C:\temp\LATTE COFFEE TEST [not found]
C:\temp\rao872 [not found]
C:\Documents and Settings\dmurthy\Desktop\aftab_cap (7572 KB)
C:\Documents and Set ... \Temporary Internet Files\OLK10\veraz041.pcap [not found]
C:\DOCUME~1\dmurthy\ ... \Zip1DDA\Zip1F33C\labxms_access_attempt.cap [not found]
C:\Documents and Set ... e_Interface_SIPMessageRouting_Iternia[1].pcap [not found]
Sample Captures
A rich assortment of example capture files on the wiki
Online
Website
Visit the project's website
User's Guide
The User's Guide (local version, if installed)
Security
Work with Wireshark as securely as possible

2. Select **Remote** from the **Interface** drop down box.



Interface: Local

cp_scvna Check Point Virtual Network Adapter (Microsoft'

Buffer size: 1 megabyte(s)

3. Enter he management IP address of the BorderNet 4000 system for the **Host**. The port number for the **Port** is 2010.

Note: The host IP address from which the trace request is triggered must be entered in the ACL without which the trace requests coming into the BorderNet 4000 will be dropped. This is a security feature. Also, remote tracing as a service should be enabled on the BorderNet 4000 SBC. See the *Dialogic® BorderNet™ 4000 SBC Configuration and Provisioning Guide* for instructions on how to create ACL entries.

4. Select **Password** authentication.
5. Enter the **Username** and **Password**. The user must have the "tracing role" assigned. Without it, the trace requests cannot be initiated. See the *Dialogic® BorderNet™ 4000 SBC Configuration and Provisioning Guide.*
6. Click **OK**.
7. If the connection is successful, the system shows the following capture options including session interfaces and recording profiles:

   Session Interface:

   - SessionIf1
   - SessionIf2
   - SessionIf3
   - SessionIf4

   Recording Profiles:

   - SignalingNoMedia
   - SignalingWithMedia
   - MediaDropped
   - FlowsDropped
8. To start a trace request choose from one of the options above.

Based on the option selected you can either enter an interface level capture filter or a message level capture filter to narrow down the trace criteria. The list below gives the valid combinations of options and filter criteria that are supported.

Option	**Supported capture filters**
SessionIf1 – SessionIf4	All IP based capture filters are supported. These are default Wireshark capture filters. For example, IP, host, port, TCP, UDP … A combination of these filters are also supported using the logical operators 'and' , 'or' and 'not'
SignalingWithMedia	Message based capture filters. For example, CallingPartyUserName, CalledPartyDomainName, IncomingInterface, IncomingPeer. Multiple Call trace Criteria can be combined using a logical operator 'and'
SignalingNoMedia	Message based capture filters. For example, CallingPartyUserName, CalledPartyDomainName, IncomingInterface, IncomingPeer. Multiple Call trace Criteria can be combined using a logical operator 'and'
MeidaDropped, FlowsDropped	No Filter required. All the dropped packets are captured even if a filter is specified.

Recording Profiles

Recording profiles help to trace sessions based on Message specific filter criteria. Each profile has a specific type of message to trace.

- SignalingNoMedia – This profile will trace all the signaling messages which match the message specific capture filter.
- SignalingWithMedia – This profile will trace all the signaling messages and RTP (media) which match the message specific capture filter.
- MediaDropped – This profile will trace all the Media packets that are dropped in the kernel. It does not require a filter.
- MediaDropped – This profile will trace all the non Media packets traffic that is dropped in the kernel. It does not require a filter.

Message Based Capture Filters

The custom Wireshark plug-in supports message based capture filters. The following message based capture filters are supported.

- CallingPartyUserPart
- CallingPartyDomain
- CallingPartyURIScheme
- CallingPartyNumber
- CalledPartyUserPart
- CalledPartyDomain
- CalledPartyURIScheme
- DialedNumber
- IncomingInterface
- IncomingPeer

Three operators are supported for matching the filters

- BeginsWith - for example, CalledPartyUserName=408%. This filter will trace all the sessions whose CalledPartyUserName begins with 408.
- EndsWith - for example, CalledPartyUserName=%9000. This filter will trace all the sessions whose CalledPartyUserName ends with 900.
- IsEqualTo - for example, CalledPartyUserName=4087509000. This filter will trace all the sessions whose CalledPartyUserName equals 4087509000.

The operators can be used with all the message based capture filters. To narrow down the traces further, any capture filters can be combined using a logical ‘and’ operation.

For example, CalledPartyUserName=408% and IncomingInterface=SIPIntf1. This will capture all the messages that arrive on SIPInterface SIPIntf1 and whose CalledPartyUserName begins with 408.

Note: Message Based Capture filters are case sensitive. The filter should exactly match the specified syntax with case.

Interface based capture filters

Interface based capture filters are used with the session options. Though Wireshark supports several interface based capture filters, only the following capture filters are qualified with the BorderNet 4000 SBC:

- IP
- TCP
- UDP
- Host
- Port
- Arp

The remaining Wireshark filters can be used to narrow down the traces. The operators and logical operations follows the Wireshark syntax.

Note: Tracing may not capture all packets when the packet traffic is too high on the interface or when system is processing a high amount of traffic. Dialogic recommends that you use specific capture filters (instead of display filters which are applied on the captured messages) to narrow down the packet traffic of interest.

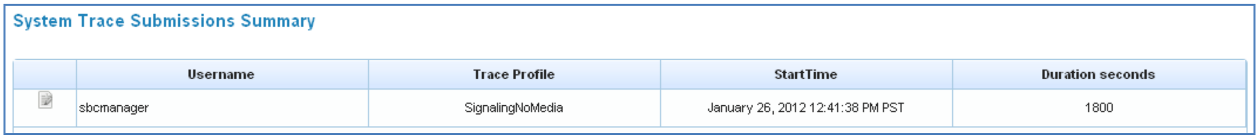
Session Tracing

You can display current sessions that are connected from Wireshark (Trace Sessions). The data displays the following:

- Wireshark trace requests in progress
- TraceProfile used for tracing
- Start time of the trace

For session traces, the TraceProfile shows the Interface and for recording profiles the trace profile shows the actual profile used. You can stop each of these traces from the WebUI. Click the **Edit** button to see the options to stop the trace. Double-click on the entry to show a detailed view of the trace request.

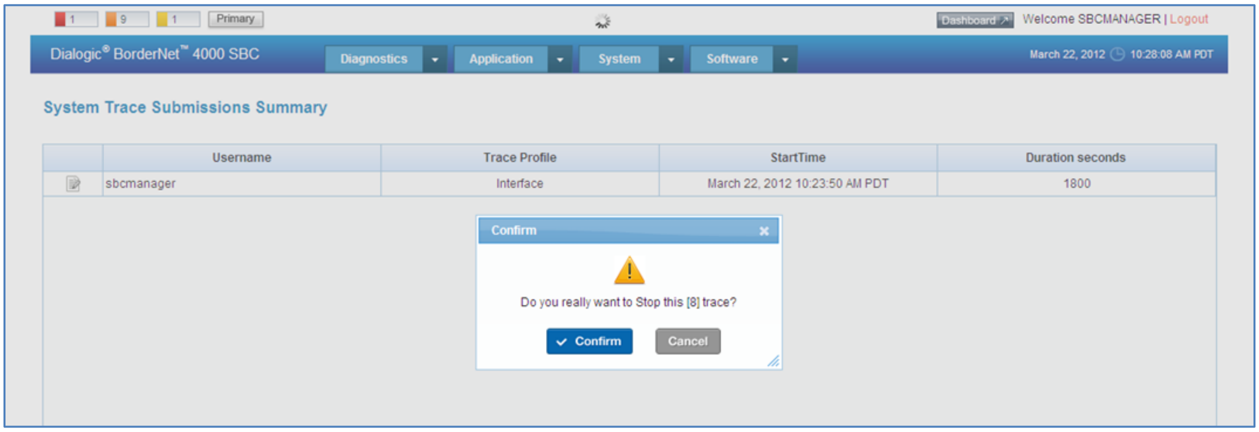
1. From the **Diagnostics** menu, select **Sessions** under **Trace**.



System Trace Submissions Summary

	Username	Trace Profile	StartTime	Duration seconds
	sbcmanager	SignalingNoMedia	January 26, 2012 12:41:38 PM PST	1800

2. To stop the session trace, select **Stop** from the edit button. Click **Confirm**.



1
9
1
Primary
Dashboard
Welcome SBCMANAGER | Logout
Dialogic® BorderNet™ 4000 SBC
Diagnostics
Application
System
Software
March 22, 2012 10:28:08 AM PDT

System Trace Submissions Summary

	Username	Trace Profile	StartTime	Duration seconds
	sbcmanager	Interface	March 22, 2012 10:23:50 AM PDT	1800

Confirm

Do you really want to Stop this [8] trace?

Media Capture

The BorderNet 4000 SBC supports media capture and recording from any connection point on the network. The GUI displays basic RTP stream characteristics, and multiple media streams can be selected and played back at any given time.

System Status

The Management System reports the following real-time system status information for the active platform on the management screen:

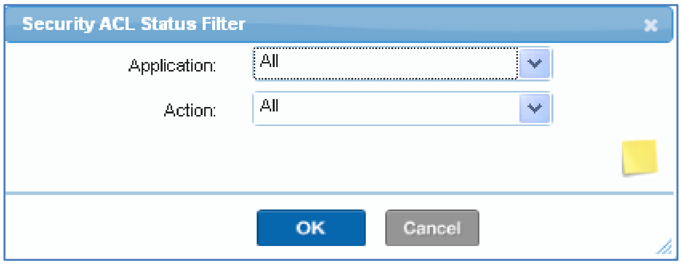
- ACL Status
- IP Route Status

Reporting ACL Status

Access Control Lists (ACLs) selectively allow or deny traffic from specified remote entities. You can create a set of static filtering rules to accept or block traffic, and BorderNet 4000 creates service specific ACLs based on other configurations. These service-aware ACLs enable fine-grain control over BorderNet 4000 traffic and prevent DoS attacks from random sources.

Follow the steps below to report the security Access Control List (ACL) Status summary.

1. From the **Diagnostics** menu, select **ACL Status** under **System Status**.

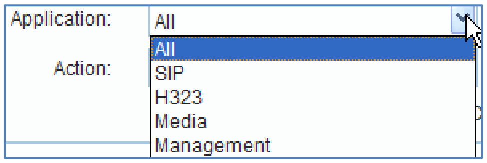


Security ACL Status Filter

Application: All

Action: All

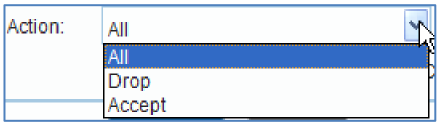
2. Select which application to report.



Application: All

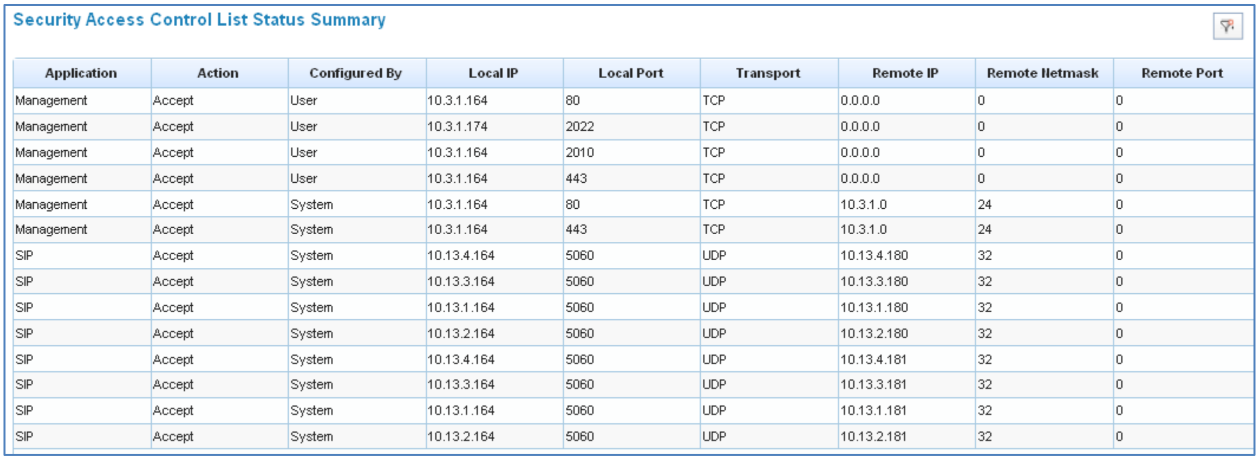
Action:

3. Select the type of ACL to report: Accept ACLs, Drop ACLs, or all ACLs.



Action: All

4. Click **OK**.

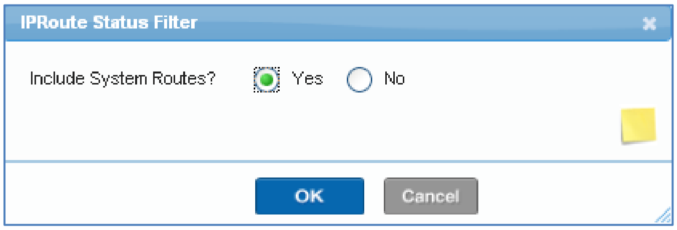


Security Access Control List Status Summary

Application	Action	Configured By	Local IP	Local Port	Transport	Remote IP	Remote Netmask	Remote Port
Management	Accept	User	10.3.1.164	80	TCP	0.0.0.0	0	0
Management	Accept	User	10.3.1.174	2022	TCP	0.0.0.0	0	0
Management	Accept	User	10.3.1.164	2010	TCP	0.0.0.0	0	0
Management	Accept	User	10.3.1.164	443	TCP	0.0.0.0	0	0
Management	Accept	System	10.3.1.164	80	TCP	10.3.1.0	24	0
Management	Accept	System	10.3.1.164	443	TCP	10.3.1.0	24	0
SIP	Accept	System	10.13.4.164	5060	UDP	10.13.4.180	32	0
SIP	Accept	System	10.13.3.164	5060	UDP	10.13.3.180	32	0
SIP	Accept	System	10.13.1.164	5060	UDP	10.13.1.180	32	0
SIP	Accept	System	10.13.2.164	5060	UDP	10.13.2.180	32	0
SIP	Accept	System	10.13.4.164	5060	UDP	10.13.4.181	32	0
SIP	Accept	System	10.13.3.164	5060	UDP	10.13.3.181	32	0
SIP	Accept	System	10.13.1.164	5060	UDP	10.13.1.181	32	0
SIP	Accept	System	10.13.2.164	5060	UDP	10.13.2.181	32	0

Reporting IP Route Status

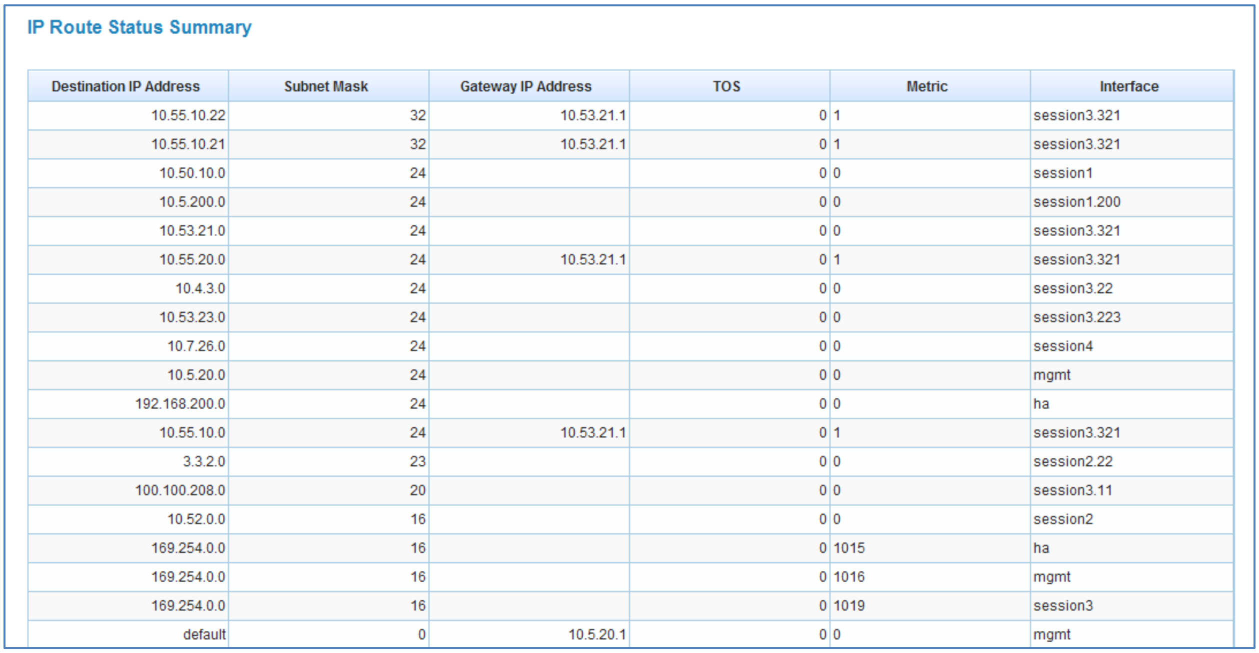
1. From the **Diagnostics** menu, select **IP Route Status** under **System Status**.



IPRoute Status Filter

Include System Routes? ● Yes ○ No

2. Select whether to report system routes or not. Routes that are automatically added by the System (for example, when VLAN Access IP addresses are configured on the system) are referred to as system added routes. This option allows you to see the routing table entries as they exists on the system. Routes that are explicitly provisioned by the operator are referred as non-system routes.
3. Click **OK**.



IP Route Status Summary

Destination IP Address	Subnet Mask	Gateway IP Address	TOS	Metric	Interface
10.55.10.22	32	10.53.21.1	0	1	session3.321
10.55.10.21	32	10.53.21.1	0	1	session3.321
10.50.10.0	24		0	0	session1
10.5.200.0	24		0	0	session1.200
10.53.21.0	24		0	0	session3.321
10.55.20.0	24	10.53.21.1	0	1	session3.321
10.4.3.0	24		0	0	session3.22
10.53.23.0	24		0	0	session3.223
10.7.26.0	24		0	0	session4
10.5.20.0	24		0	0	mgmt
192.168.200.0	24		0	0	ha
10.55.10.0	24	10.53.21.1	0	1	session3.321
3.3.2.0	23		0	0	session2.22
100.100.208.0	20		0	0	session3.11
10.52.0.0	16		0	0	session2
169.254.0.0	16		0	1015	ha
169.254.0.0	16		0	1016	mgmt
169.254.0.0	16		0	1019	session3
default	0	10.5.20.1	0	0	mgmt

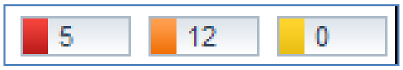
Real-Time Status and Performance

All functionalities are accessible through the WebUI.

Alarms

On the WebUI, three color coded boxes at the top displays the number of current alarms in three categories:

- Critical - Red
- Major - Orange
- Minor - Yellow



Each of these boxes represent the numbers of outstanding alarms by severity. Periodic refreshing these alarm numbers indicates ongoing alarm notification for the operator's visibility. See the Troubleshooting chapter for an explanation of alarms and corrective actions.

Dashboard

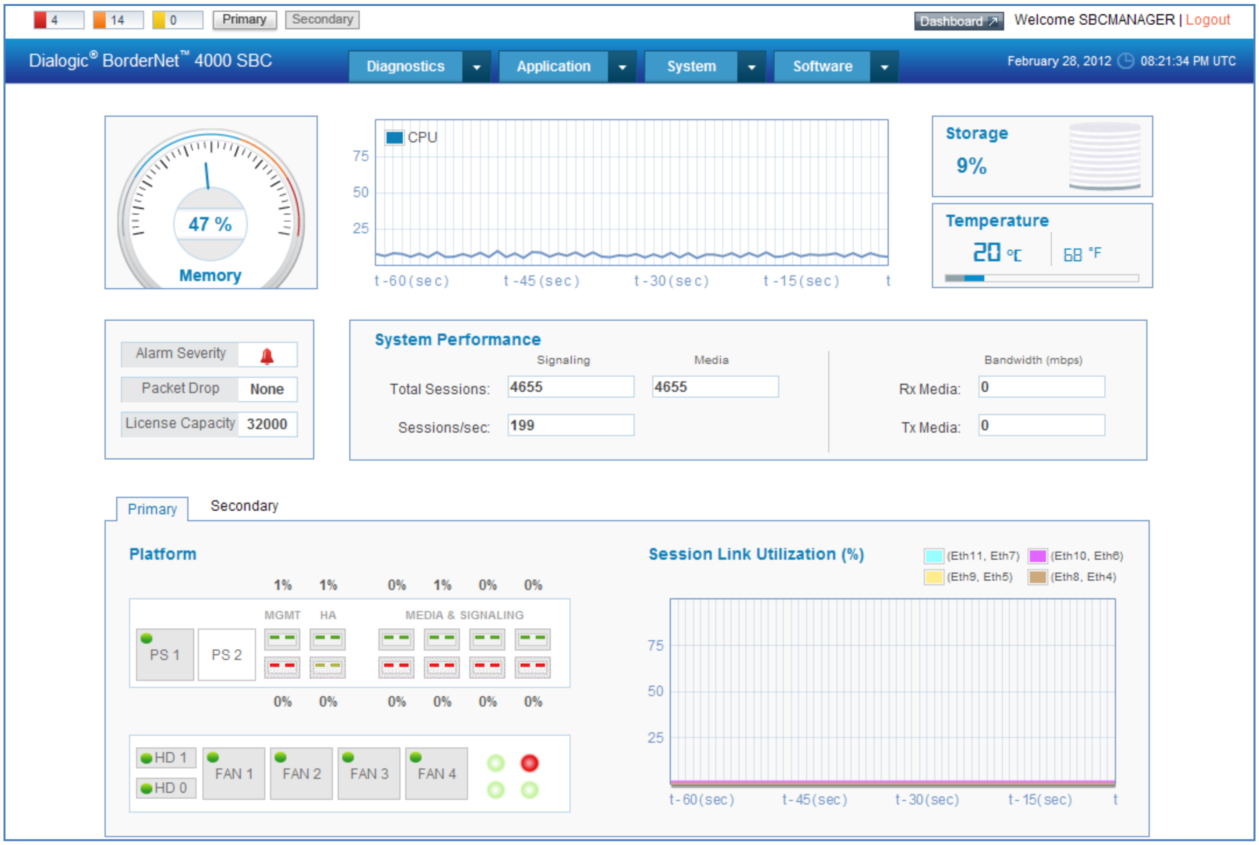
The dashboard provides real-time information on how BorderNet 4000 SBC is functioning including the platform status and system performance above including the following:

- Current alarms (color-coded by severity).
- Real-time charts on the last 60 seconds of CPU and memory usages
- Hardware component status
- Memory Utilization
- Storage utilization and thermal status
- Current total number of live signaling and media sessions
- Current processing rate (in calls per second)
- Status and usage level at each network interface

Follow the step below to display the dashboard:

1. Click **Dashboard** from the WebUI.

2. The following screen appears.



Alarm Severity	
Packet Drop	None
License Capacity	32000

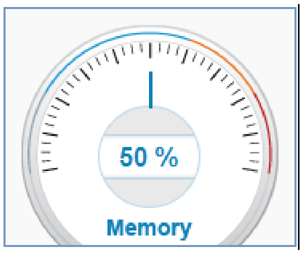
System Performance

	Signaling	Media
Total Sessions:	4655	4655
Sessions/sec:	199	

Bandwidth (mbps)	
Rx Media:	0
Tx Media:	0

The sections below describe each part of the dashboard.

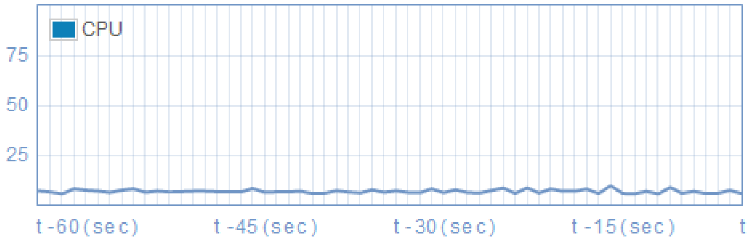
Memory



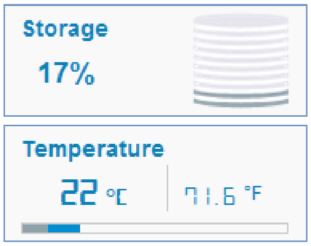
The Memory utilization dial on the dashboard gives the percentage of total memory allocated to the application. Memory is statically allocated in BorderNet 4000 which means that application memory consumption does not increase drastically as an increasing number of calls flow through the BorderNet 4000 SBC. Similarly, there is memory allocation even when the system is not having any traffic flow. When utilization goes beyond 90 percent or if the utilization is varying in real time, then operator would need to run other diagnostics to find out the cause.

CPU Usage

The chart below displays the last 60 seconds of CPU activity and bandwidth.



Storage and Temperature



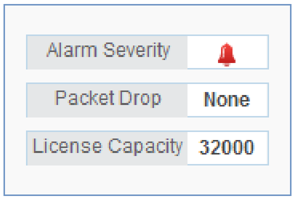
Storage
17%

Temperature
22 °C | 71.6 °F

The Storage indicates the disk space usage as a percentage. The Image is made up of 10 bands. When storage exceeds 70% capacity, it changes the color of the exceeded space (above 70) to orange. When it exceeds 80%, exceeded space is represented in red to get the operator's attention. For example, if storage space consumption is 85%, the eighth band is shown in orange and the ninth band is shown in red.

Temperature is shown in both Centigrade and Fahrenheit. The band at the bottom is color coded. When it goes up to the warning threshold, the band shows the exceeded range in orange. At critical threshold, the band color shows the exceeded value in red to get operator attention

Alarm Severity, Packet Drop, License Capacity



Alarm Severity	🔔
Packet Drop	None
License Capacity	32000

The Alarm Severity indicates the highest level of alarm found in the system. For example, if there are zero outstanding critical alarms (red), two major alarms (orange) and five minor alarms (yellow), then dashboard would show an orange alert.

The Packet Drop indicates the level of discarded Ethernet packets in the system. It has the following three levels.

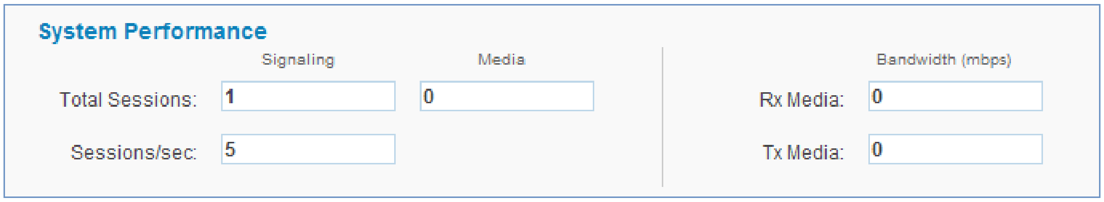
- **None** – 0-10 percent packets being dropped
- **Low** – 10-25 percent packets being dropped
- **High** – greater than 25 percent being dropped

License Capacity indicates the number of sessions licensed. When the number of concurrent sessions in the system exceed 80% of license capacity, this number turns to Orange. When the threshold increases beyond 90%, the License Capacity turns red.

System Performance

The Management System reports real-time performance information for the active platform at the system level:

- Total Sessions: Signaling and Media
- Incoming Session Rate
- System Bandwidth Consumption for Media



System Performance

	Signaling	Media		Bandwidth (mbps)
Total Sessions:	1	0	Rx Media:	0
Sessions/sec:	5		Tx Media:	0

Total Sessions Signaling represents the count of all the calls which are attempted, not necessarily answered.

Total Sessions Media represents all answered calls for which the BorderNet 4000 SBC does media interception.

Sessions/sec is the number of new incoming session attempts per second across all session interfaces.

Media Bandwidth (in Mbps) indicates system level media bandwidth utilization (transmit and receive) across all session interfaces. For example, on a system with 4 GigE interfaces in Full Duplex mode, Rx and Tx can each show values closer to 4096 Mbps. However, signaling packets and other dropped packets are not considered for this usage representation. As stated, it is representative of RTP stream only.

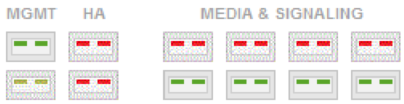
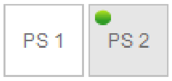
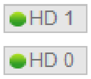
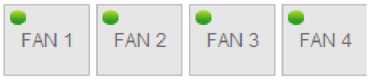
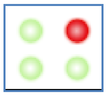
Platform Status

The WebUI reports the following real-time platform status information for the active platform.

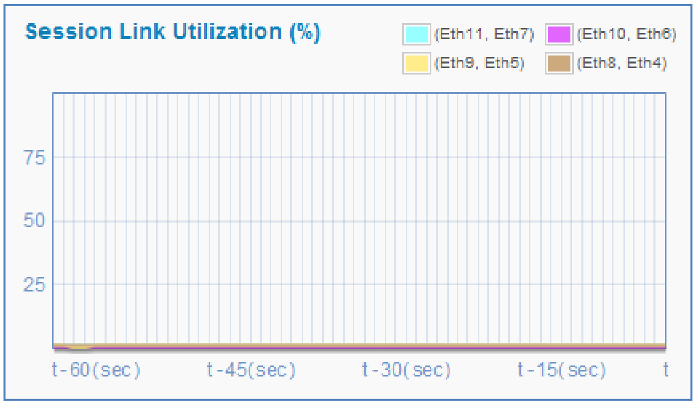
Note: You can toggle the view between the Active and Secondary platforms.

The color coding for the LEDs are as follows:

- Red – Down
- Gray – Not configured or disabled
- Green – Up or active

Component	Supported Status
Management, High Availability, and Media and Signaling Links 	• Dark green: Active • Pale Green: Standby • Red: Down • Gray: Not Configured
Power Supplies 	• Green: Functional • Red: Non-functional or down • White: Not installed
Hard Disks 	• Green: Functional • Red: Non-functional or down • White: Not installed
Fans 	• Green: Functional • Red: Non-functional or down • White: Not installed
Integrated Platform Status LEDs 	**Top left:** M-Fault indicates a major fault warning, such as if a component temperature reaches a critical reading. **Top right:** P-Fault indicates a power supply fault. This LED illuminates if a fault occurs with a fan, temperature, or voltage reading associated with the power supply. **Bottom left:** C-Fault indicates a critical, non-recoverable event. The BorderNet 4000 SBC will perform a graceful shutdown to protect components from thermal damage. **Bottom right:** Not currently used.

Session Link Utilization

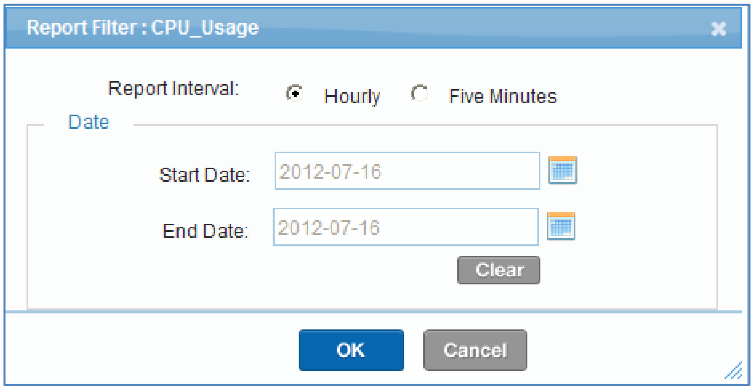


The Session Link Utilization percentage provides a graphical representation of all four session interfaces in the system. It captures utilization every second and graphs it over a one minute time interval. If a session link is set to 1 Gbps and if it carries a traffic of 500 Mbps, the utilization is represented as 50%.

Reporting CPU Utilization

Follow the steps below to report CPU utilization:

1. From the **Diagnostics** menu, select **CPU Usage** under the **System Performance** section.


Report Filter : CPU_Usage

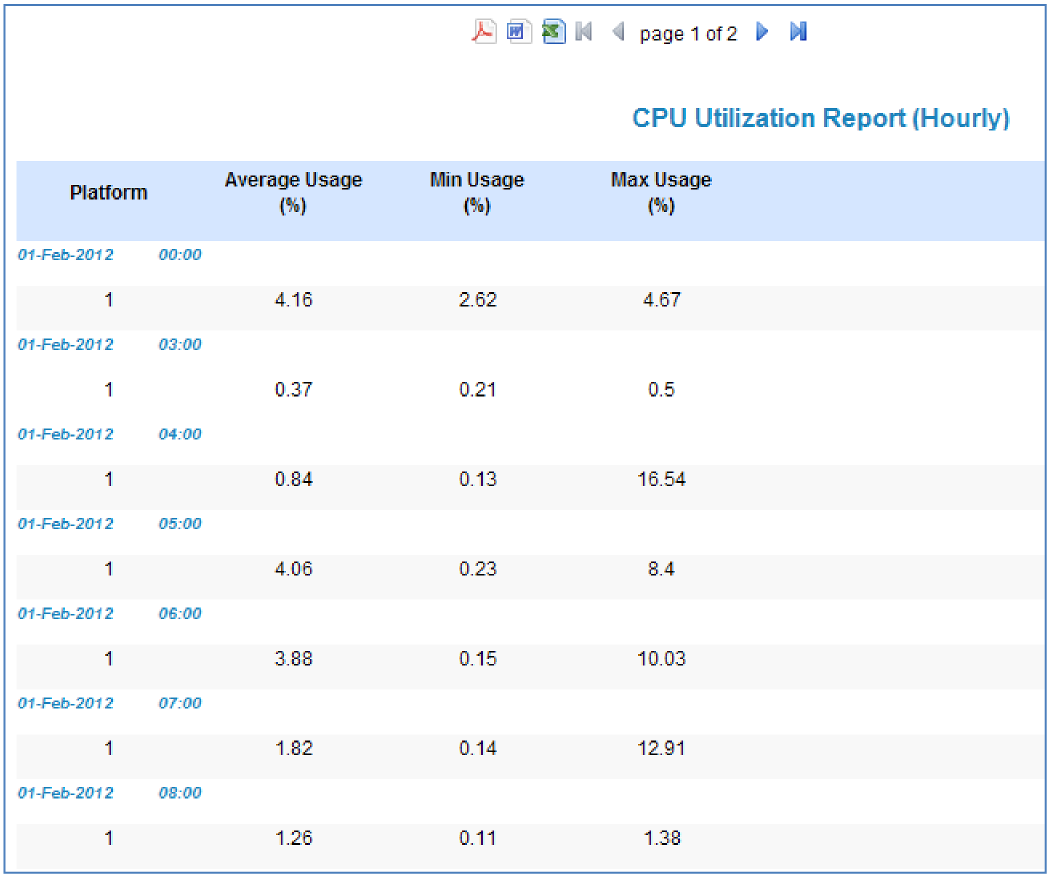
Report Interval: ● Hourly ○ Five Minutes

Date

Start Date: 2012-07-16

End Date: 2012-07-16

2. Select whether you want to report the CPU Utilization hourly or five minute intervals.
3. Select the Start Date and End Date of the period that you want to report CPU Utilization.
4. Click **OK** and the following appears.



CPU Utilization Report (Hourly)

Platform	Average Usage (%)	Min Usage (%)	Max Usage (%)
01-Feb-2012	*00:00*		
1	4.16	2.62	4.67
01-Feb-2012	*03:00*		
1	0.37	0.21	0.5
01-Feb-2012	*04:00*		
1	0.84	0.13	16.54
01-Feb-2012	*05:00*		
1	4.06	0.23	8.4
01-Feb-2012	*06:00*		
1	3.88	0.15	10.03
01-Feb-2012	*07:00*		
1	1.82	0.14	12.91
01-Feb-2012	*08:00*		
1	1.26	0.11	1.38

Software Management

This section explains how to perform the following:

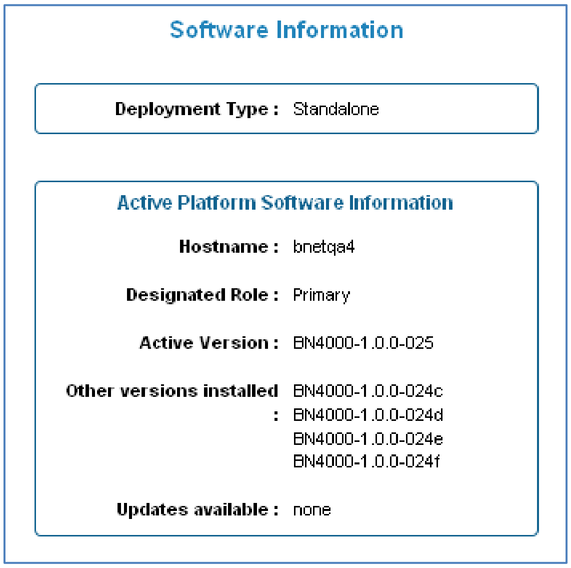
- Displaying software information
- Uploading new software
- Upgrading software
- Rolling back software
- Backing up and restoring configuration data

Displaying Software Information

There can be a maximum of five versions installed on the platform.

Follow the step below to display software information.

1. From the **Software** menu, select **About**. For standalone deployments the following screen appears:



Software Information

Deployment Type : Standalone

Active Platform Software Information

Hostname : bnetqa4

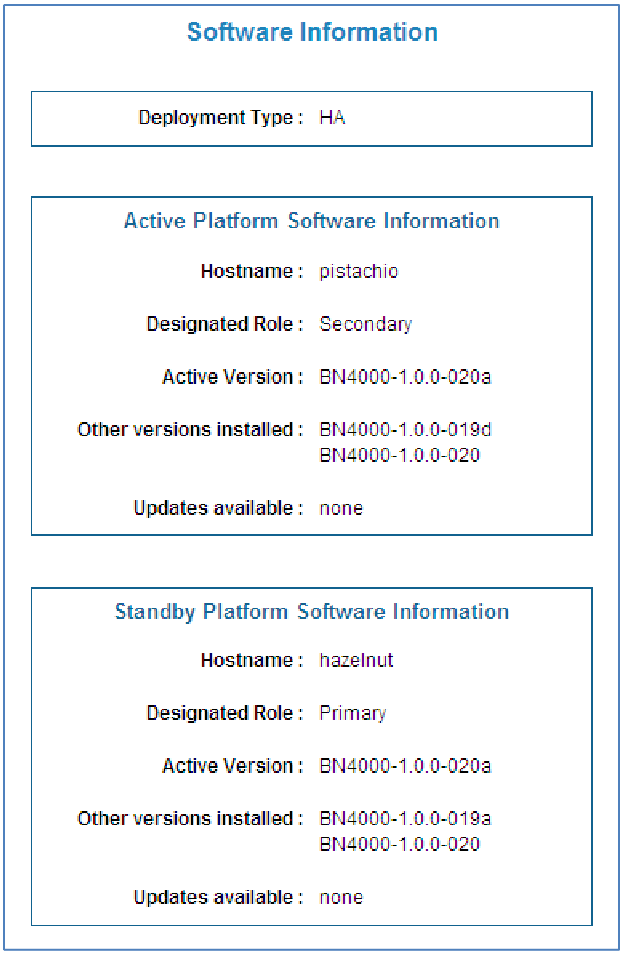
Designated Role : Primary

Active Version : BN4000-1.0.0-025

Other versions installed : BN4000-1.0.0-024c
BN4000-1.0.0-024d
BN4000-1.0.0-024e
BN4000-1.0.0-024f

Updates available : none

For HA systems, the following screen appears:



Software Information

Deployment Type : HA

Active Platform Software Information

Hostname : pistachio

Designated Role : Secondary

Active Version : BN4000-1.0.0-020a

Other versions installed : BN4000-1.0.0-019d
BN4000-1.0.0-020

Updates available : none

Standby Platform Software Information

Hostname : hazelnut

Designated Role : Primary

Active Version : BN4000-1.0.0-020a

Other versions installed : BN4000-1.0.0-019a
BN4000-1.0.0-020

Updates available : none

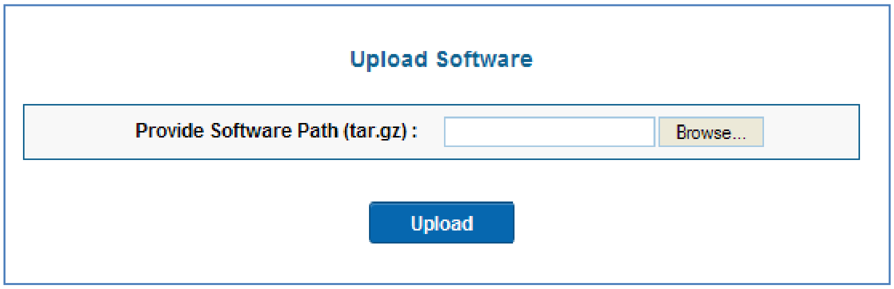
Uploading a New Software Release

You can upload a new release to the system. In an HA deployment, the software upload is done only once and it is synched automatically to the standby platform.

Uploaded software releases are cleaned up automatically. Only the last three releases are kept on the system.

Follow the steps below to upload a new software release.

1. From the **Software** menu, select **Upload New Release**. The following screen appears.



Upload Software

Provide Software Path (tar.gz) :

2. Click **Browse...** to select the file for upload.
3. Click **Upload** to upload the software.

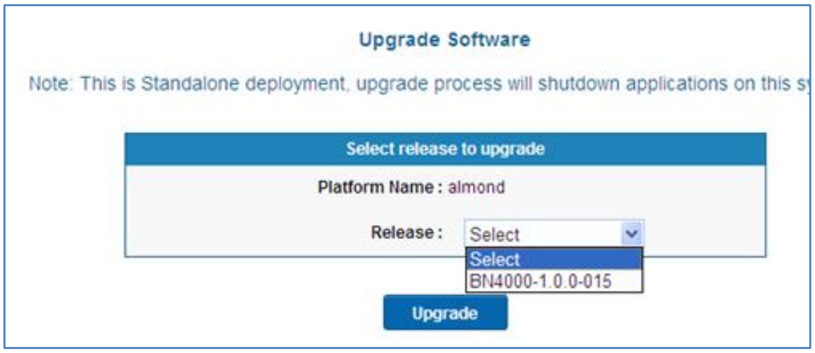
Upgrading Software

The following applies to upgrading software:

- In a standalone deployment, you must upgrade software during a maintenance window because it affects traffic.
- All application processes are shutdown during the upgrade process.
- Application services are started as soon as the upgrade is completed.
- In an HA deployment, the upgrade is allowed only on the standby platform.
- The following operations should be done for HA deployment upgrade:
    - Upgrade current standby platform
    - Failover
    - Upgrade current standby platform

Follow the steps below to upgrade the current software version.

1. From the **Software** menu, select **Upgrade**. In a standalone deployment, the following screen appears.



Upgrade Software

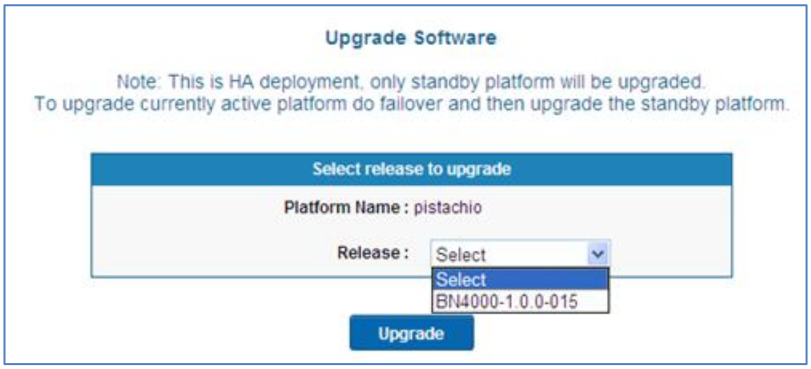
Note: This is Standalone deployment, upgrade process will shutdown applications on this sy

Select release to upgrade

Platform Name : almond

Release : Select

In an HA deployment, the following screen appears:



Upgrade Software

Note: This is HA deployment, only standby platform will be upgraded.
To upgrade currently active platform do failover and then upgrade the standby platform.

Select release to upgrade

Platform Name : pistachio

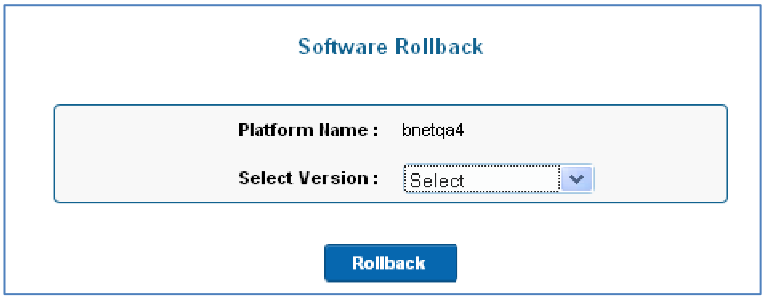
Release : Select

2. Select the software release and click **Upgrade**.

Rolling Back Software

Follow the steps below to roll back the software to a previous release:

1. From the **Software** menu, select **Rollback**.



Platform Name : bnetqa4

Select Version : Select

2. Select the software version to roll back to and click **Rollback**.

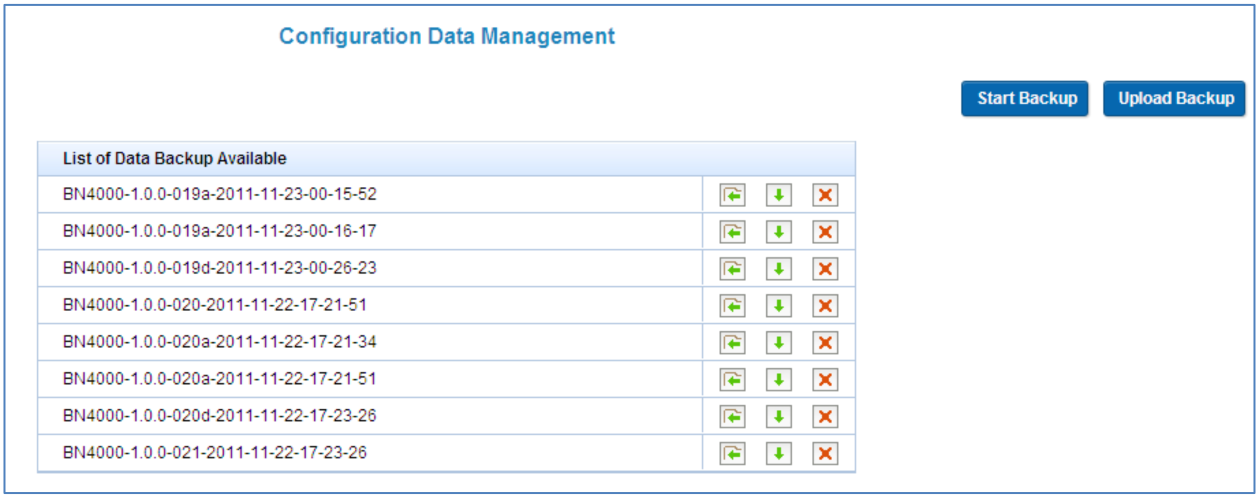
Restoring and Backing Up Configuration Data

Backing up software differs on a standalone system and an HA system as follows:

- On a standalone system, when you back up the configuration data, the provisioning process is shut down. It is started up once the backup is completed.
- On an HA system, configuration data backup is taken on a standby platform and is also transferred to the active platform automatically.

Follow the steps below to back up and restore configuration data:

1. From the **Software** menu, select **Backup & Restore** under **Data Management**. The follow screen appears.



List of Data Backup Available			
BN4000-1.0.0-019a-2011-11-23-00-15-52	⇦	↓	✕
BN4000-1.0.0-019a-2011-11-23-00-16-17	⇦	↓	✕
BN4000-1.0.0-019d-2011-11-23-00-26-23	⇦	↓	✕
BN4000-1.0.0-020-2011-11-22-17-21-51	⇦	↓	✕
BN4000-1.0.0-020a-2011-11-22-17-21-34	⇦	↓	✕
BN4000-1.0.0-020a-2011-11-22-17-21-51	⇦	↓	✕
BN4000-1.0.0-020d-2011-11-22-17-23-26	⇦	↓	✕
BN4000-1.0.0-021-2011-11-22-17-23-26	⇦	↓	✕

2. This screen shows the list of configuration data backups available on the system. You can do the following from this screen:
   - Start Backup
   - Restore Backup
   - Download Backup
   - Delete Backup
   - Upload Backup

Starting the Backup

1. Click **Start Backup** to backup the configuration data.
2. Click **Confirm**.

Restoring the Backup

Note: Restoring configuration data is a service impacting action.

The process for restoring configuration data differs on a standalone system and an HA system as follows:

- On a standalone system, when you are restoring data, application services are shutdown and started once the backup restoration is complete.
- On an HA system, you restore data on the standby platform and then the automatic failover happens. You do not have to restore data on both platforms.

Note: The system that you are restoring the data to has to be on the same version as what was backed up. In addition, the filename has to be the same as the original filename that was downloaded.

1. Click ↩ to restore the configuration data backup.
2. Click **Confirm**.

Downloading the Backup

1. Click ⬇ to download the configuration data to the local machine.
2. Click **Confirm**.

Deleting the Backup

1. Click ✖ to delete the configuration data backup.
2. Click **Confirm.**

Uploading the Backup

Click the **Upload Backup** button to upload the configuration data backup file from the local machine to the BorderNet 4000 application platform.

Audit Logs

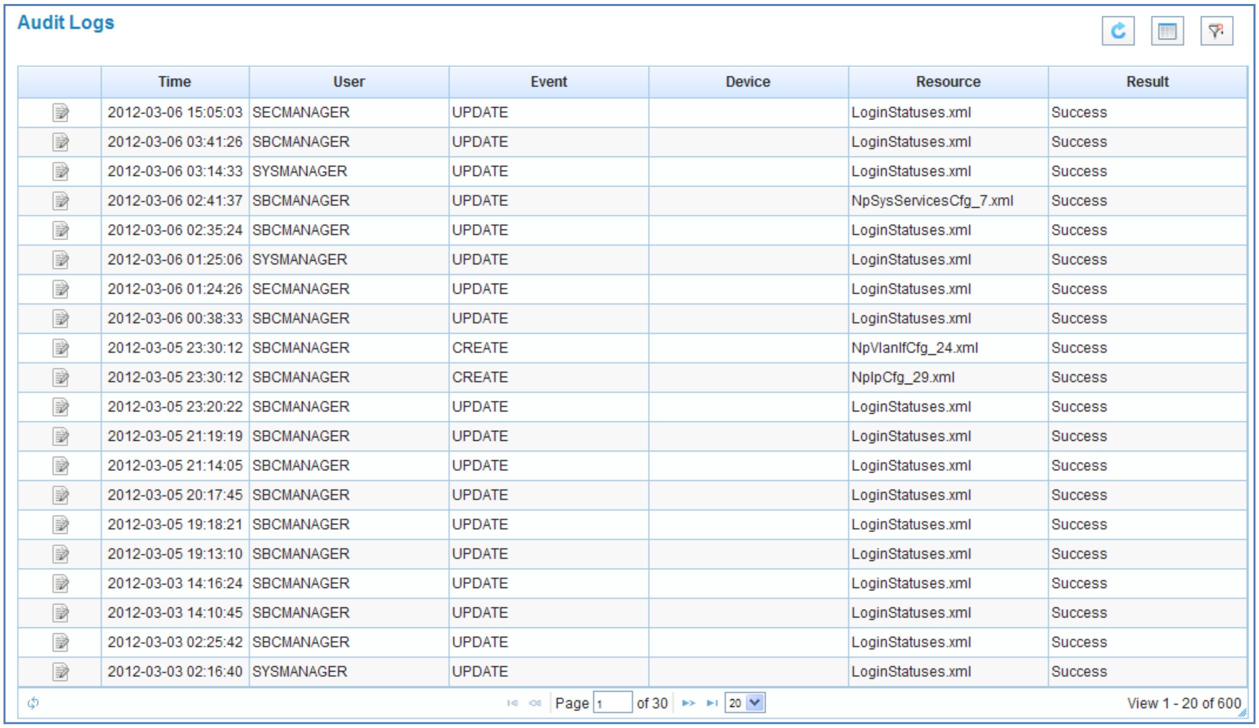
The Audit Logging functionality audits every data change happening in the system and writes the information into an audit record file. The system maintains the file for one year The following audit records are recorded into the file:

Time	Date-time	N	Date+Time in seconds when the audit trail is generated.
Username	String	N	Name of the user who requested the change.
Device	String	Y	IP address or device name from where WebUI was accessed.
Event	String	N	CREATE, UPDATE, DELETE
Resource	String	N	Name of the resource/filename that was modified.
Result	String	N	Success/Failure

Note: You must have Security Auditor privileges to view the audit records.

Viewing Audit Logs

1. From the **System** menu, select **Audit Logs** under **Administration**.

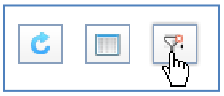


Audit Logs

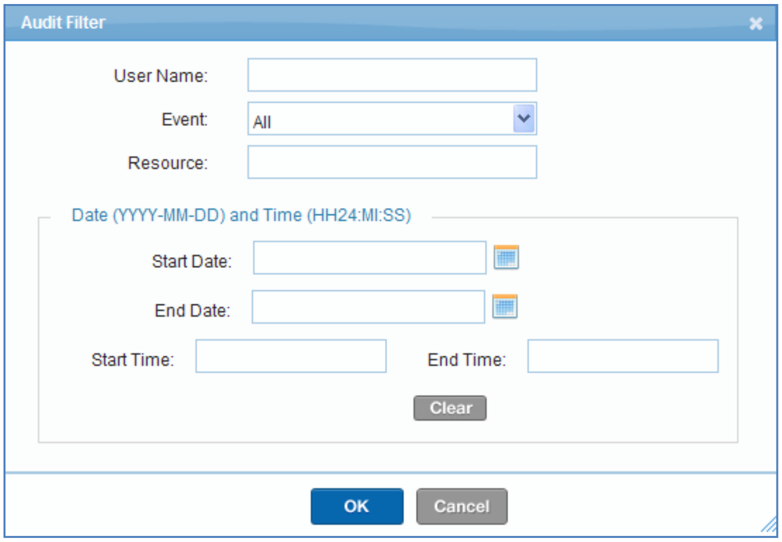
	Time	User	Event	Device	Resource	Result
	2012-03-06 15:05:03	SECMANAGER	UPDATE		LoginStatuses.xml	Success
	2012-03-06 03:41:26	SBCMANAGER	UPDATE		LoginStatuses.xml	Success
	2012-03-06 03:14:33	SYSMANAGER	UPDATE		LoginStatuses.xml	Success
	2012-03-06 02:41:37	SBCMANAGER	UPDATE		NpSysServicesCfg_7.xml	Success
	2012-03-06 02:35:24	SBCMANAGER	UPDATE		LoginStatuses.xml	Success
	2012-03-06 01:25:06	SYSMANAGER	UPDATE		LoginStatuses.xml	Success
	2012-03-06 01:24:26	SECMANAGER	UPDATE		LoginStatuses.xml	Success
	2012-03-06 00:38:33	SBCMANAGER	UPDATE		LoginStatuses.xml	Success
	2012-03-05 23:30:12	SBCMANAGER	CREATE		NpVlanIfCfg_24.xml	Success
	2012-03-05 23:30:12	SBCMANAGER	CREATE		NpIpCfg_29.xml	Success
	2012-03-05 23:20:22	SBCMANAGER	UPDATE		LoginStatuses.xml	Success
	2012-03-05 21:19:19	SBCMANAGER	UPDATE		LoginStatuses.xml	Success
	2012-03-05 21:14:05	SBCMANAGER	UPDATE		LoginStatuses.xml	Success
	2012-03-05 20:17:45	SBCMANAGER	UPDATE		LoginStatuses.xml	Success
	2012-03-05 19:18:21	SBCMANAGER	UPDATE		LoginStatuses.xml	Success
	2012-03-05 19:13:10	SBCMANAGER	UPDATE		LoginStatuses.xml	Success
	2012-03-03 14:16:24	SBCMANAGER	UPDATE		LoginStatuses.xml	Success
	2012-03-03 14:10:45	SBCMANAGER	UPDATE		LoginStatuses.xml	Success
	2012-03-03 02:25:42	SBCMANAGER	UPDATE		LoginStatuses.xml	Success
	2012-03-03 02:16:40	SYSMANAGER	UPDATE		LoginStatuses.xml	Success

Page 1 of 30 20 View 1 - 20 of 600

2. Click the filter button to refine the results:



3. Enter the filtering from the screen below:



Audit Filter

User Name:

Event: All

Resource:

Date (YYYY-MM-DD) and Time (HH24:MI:SS)

Start Date:

End Date:

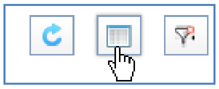
Start Time: End Time:

Clear

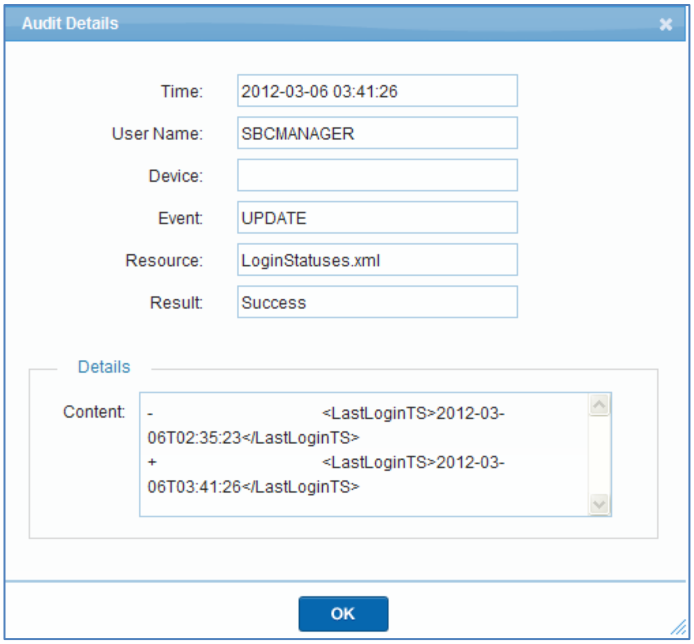
OK Cancel

Note: The **User Name** and **Resources** fields are case-sensitive.

4. To display the details on a record, select the record and click the audit button.



You can also double-click any record to display the audit details.



Audit Details

Time:	2012-03-06 03:41:26
User Name:	SBCMANAGER
Device:	
Event:	UPDATE
Resource:	LoginStatuses.xml
Result:	Success

Details

Content:

```
-                    <LastLoginTS>2012-03-
06T02:35:23</LastLoginTS>
+                    <LastLoginTS>2012-03-
06T03:41:26</LastLoginTS>
```

Troubleshooting

This section help you determine the cause of a problem with the BorderNet 4000 SBC and includes corrective actions to follow.

Alarms

The table below lists each alarm that the BorderNet 4000 SBC produces along with descriptions and corrective actions.

Name	Category	Severity	Description	Corrective Actions
Ethernet Link Failed	Network	Critical	Raised when the system detects the Ethernet link (both Primary and Secondary Ethernet links of the link pair) to have failed.	Check both the physical interfaces for the given Ethernet link and ensure they are properly connected to the switch. If the problem persist check the cables and the Ethernet properties such as speed, duplex, auto negotiation is configured same on both ends of the Ethernet link.
Physical Ethernet Interface Failed	Network	Major	The system detects the physical interface failure.	Check the physical interfaces and ensure they are properly connected to the switch. If the problem persist check the cables and the Ethernet link properties such as speed, duplex, auto negotiation is configured same on both ends of the Ethernet link.
Interface Activation Failed	Configuration	Critical	The system failed to open up a listening ip:port for the configured interfaces.	Check the interface configuration on the WebUI. Turn-off and Turn-on the configuration Remove Associations. Clone and delete old….rename the clone to the previous one (source). On the interface screen, sort on the IP and ensure the same IP and port does not exist. Restart IBCF service.
Registration with Gatekeeper failed	Configuration	Critical	The H.323 Interface failed to register with the Gatekeeper Peer.	Check the accuracy of the Gatekeeper information on the

Name	Category	Severity	Description	Corrective Actions
				respective Peer. Check availability of the gatekeeper from the BorderNet 4000 interface Turn Off and On the interface to reinitiate registration.
Configuration Data Validation Failure	Configuration	Critical	When the platform becomes active from standby, the configuration data is validated. If the validation fails then this alarm is raised.	Follow the detail error message in the alarm, and delete the objects that caused the validation to fail, and restart the platform. Delete the object that caused the problem. Then restart the platform.
Link Disabled	Configuration	Minor	Raised when the Ethernet link is administratively "disabled". The alarm gets cleared when this Ethernet link is administratively "Enabled".	The alarm is the result of user action disabling the link. User can enable the link from Ethernet Links Screen.
Configuration Data Validation Failure	Configuration	Critical	When the platform becomes active from standby, the configuration data is validated. If the validation fails then this alarm is raised.	Follow the detail error message in the alarm, and delete the objects that caused the validation to fail, and restart the platform. Delete the object that caused the problem. Then restart the platform.
Ethernet Link Administratively Disabled	Configuration	Minor	Raised when the Ethernet link is administratively "disabled". The alarm gets cleared when this Ethernet link is administratively "Enabled".	The alarm is the result of user action disabling the link. User can enable the link from Ethernet Links Screen.
IP Address Configuration Failure	Configuration	Minor	The received configuration failed to get configured/ applied on the BorderNet 4000 SBC platform. The following are the configuration failure examples that could result in this alarm: - IP Address assignment/un-assignment failure. The FDN and additional	The operator provided a configuration of the IP Address, IP Route etc. that was rejected by the underlying OS layer. This may happen when the given configuration is either not valid or already exists or conflicts with another configuration on the platform.

Name	Category	Severity	Description	Corrective Actions
			alarm details contains the information for the object type (for example, VLAN,IP, and IPROUTE) and the object identified (for example. Id or the Name of the object) that failed to get configuration on the platform.	The additional detail string in the alarm usually provides the error not received from the operating system which can be used to further debug the issues with the configuration data. The operator should check and correct/remove the invalid configuration data from the invalid configuration data from the provisioning system and manually clear the alarm.
IP Route Configuration Failure	Configuration	Minor	The received configuration failed to get configured/ applied on the BorderNet 4000 SBC platform. The following are the configuration failure examples that could result in this alarm: - IPROUTE configuration failure. The FDN and additional alarm details contains the information for the object type (for example, VLAN,IP, and IPROUTE) and the object identified (for example, Id or the Name of the object) that failed to get configuration on the platform.	The operator provided a configuration of IP Address, IP Route etc. that was rejected by the underlying OS layer. This may happen when the given configuration is either not valid or already exists or conflicts with another configuration on the platform. The additional detail string in the alarm usually provides the error not received from the operating system which can be used to further debug the issues with the configuration data. The operator should check and correct/remove the invalid configuration data from the provisioning system and manually clear the alarm.
VLAN Configuration Failure	Configuration	Critical	The received configuration fails to get configured and applied on the BorderNet 4000 platform. VLAN addition/ deletion is a configuration failure that could result in this alarm. The FDN and additional	The operator provided a configuration of VLAN that was rejected by the underlying OS layer. This may happen when the given configuration is either not valid or already exists or conflicts with other configuration on the platform. The additional detail string in the alarm

Name	Category	Severity	Description	Corrective Actions
			alarm details contains the information for the object type (e.g. VLAN,IP, IPROUTE etc.) and the object identified (e.g. Id or the Name of the object) that failed to get configuration on the platform.	usually provides the error not received from the operating system which can be used to further debug the issues with the configuration data. The operator should check and correct/remove the invalid configuration data from the provisioning system and manually clear the alarm.
Session Data Record Disabled in Configuration	Configuration	Major	When the Session Detail Record (SDR) is disabled, no SDR records are generated while both signaling and media traffic are on-going.	To enable the Session Detail Record, select **SDR Configuration** from the System menu. Select **Enable**.
Peer Blacklisted Due to Packet Rate	Security	Major	A particular peer gets more packets than configured and entered into the Blacklist.	Verify with Security Profile and Reports (peer-level statistics will be needed) Operator should first check if this is the desired behavior. If it is, then monitor to see if the peer is removed from blacklist after the timeout; otherwise, the dynamic blacklisting can be re-configured.
Peer Blacklisted - Due to Exceeded Session Rate or Malformed Messages	Security	Major	The system received a high session rate - more than configured. The system received malformed SIP messages from a peer - more than allowed so it is blacklisted.	Verify with the Security Profile and Reports (peer-level statistics will be needed). First check if this is the desired behavior. If it is, then monitor to see if the peer is removed from the blacklist after the timeout; otherwise, the dynamic blacklisting can be re-configured.
Excessive Packet Drops	Security	Minor	Too many packets are being dropped in the system.	Verify the System Statistics. This is an indicative alarm and no correction required.
TLS Connectivity to Un-Configured	Security	Minor	The TLS handshake with the remote unconfigured	Verify the certificates

Name	Category	Severity	Description	Corrective Actions
Peer Failed			peer failed.	and cipher suites configured on the TLS profile for the interface used to connect to this peer.
TLS Connectivity to Configured Peer Failed	Security	Minor	The TLS handshake with the remote configured peer fails.	Verify the certificates and cipher suites configured on the TLS profile for the interface used to connect to this peer.
Maximum Active Sessions reached on Peer	QoS	Major	Calls were rejected at the Peer due to exceeding the configured Max Active Sessions at the Peer in the security profile.	Verify the Security Profile and Reports. Check the security profile.
Maximum Active Sessions reached on Interface	QoS	Major	Calls were rejected at the Interface due to exceeding the configured Max Active Sessions at the Interface in the security profile.	Verify the Security Profile and Reports. Check the security profile.
Maximum Outgoing Active Sessions Reached on Peer	QoS	Major	The outgoing sessions at a peer exceeded the maximum outgoing limit allowed at the peer.	Verify the Security Profile and Reports. Check the security profile.
Maximum Outgoing Active Sessions reached on Interface	QoS	Major	The outgoing sessions at an interface exceeded the maximum outgoing limit allowed at the interface.	Verify the Security Profile and Reports. Check the security profile.
Maximum Incoming Active Sessions Reached on Peer	QoS	Major	Incoming sessions at a peer exceeded the maximum incoming limit allowed at the peer.	Verify the Security Profile and Reports. Check the security profile.
Maximum Incoming Active Sessions Reached on Interface	QoS	Major	Incoming sessions at an interface exceeded the maximum incoming limit allowed at the interface.	Verify the Security Profile and Reports. Check the security profile.
Maximum Outgoing Session Rate Reached on Peer	QoS	Major	The rate of rejection for the outgoing calls exceeded 10% of the maximum outgoing rate at the peer.	Verify the Security Profile and Reports. Check the security profile.
Maximum Outgoing Session Rate reached on Interface	QoS	Major	The rate of rejection for the outgoing calls exceeds 10% of the maximum outgoing rate	Verify the Security Profile and Reports. Check the security profile.

Name	Category	Severity	Description	Corrective Actions
			at the Interface.	
Maximum Incoming Sessions Rate Reached on Peer	Qos	Major	The rate of rejection for the incoming calls exceeded 10% of the maximum incoming rate at the peer.	Verify the Security Profile and Reports. Check the security profile.
Maximum Incoming Sessions Rate Reached on Interface	QoS	Major	The rate of rejection for the incoming calls exceeded 10% of the maximum incoming rate at the Interface.	Verify the Security Profile and Reports. Check the security profile.
High Packet Rate At Peer	QoS	Minor	A peer received more than the configured packet rate.	Verify the Security Profile and Reports.
High Packet Rate At Interface	QoS	Minor	An interface receives more than the configured Packet rate.	Verify with Security Profile and Reports.
Connectivity Failure with Peer	QoS	Major	A configured peer fails to respond to OPTIONS sent by the system.	If calls can be sent over that peer regardless then turn-off connectivity for that peer. If the peer is supposed to respond verify that if there are routes to the peer. Also see if routes to that peer need to determined. Verify that what is configured from WebUI has made it properly to the internal components by another debug mechanism. See if there are any configuration errors if any. See if there are internal configuration errors by intrusive debugging into the platform such as debug access on process, and logs.
Packet Rate Limit Exceeded at Peer	QoS	Minor	Indicative alarm. Peer received more than the configured packet rate.	No corrective action
Packet Rate Limit Exceeded at	QoS	Minor	Indicative alarm Peer received more than	No corrective action

Name	Category	Severity	Description	Corrective Actions
Interface			the configured packet rate.	
Bandwidth Exceeded at Network Interface	Overload	Critical	Bandwidth at the network interface level is exhausted as computed from the session capacity.	Verify from reports if there are peers that are generating more traffic than they should and if configurations are accurate. Traffic generating peers on the network interface level can be reconfigured or locked to avoid traffic.
Session License Limit Reached	Overload	Critical	The number of concurrent sessions reached the licensed limit.	
CPU Utilization Reached Overload Level	Overload	Major, Minor, Critical	The CPU usage crossed a predefined threshold. The severity changes based on the threshold crossed.	
CPU Utilization Reached Overload Level	Overload	Minor/Major/Critical	This alarm is raised if CPU usage crosses a predefined threshold. The severity changes based on the threshold crossed.	
License Expired	License	Critical	Indicates either that the trial/production license has expired.	Verify the License Contents on WebUI and purchase an updated new license.
License Nearing Expiry	License	Critical	Indicates either that the trial/production expiry is nearing (15 days prior).	Verify the License Contents on WebUI and purchase an updated new license.
Lost Communication with Peer Platform	HA	Critical	Raised when the platform deployed in HA configuration detects communication failure with paired platform.	Check the connectivity between the paired platforms of the HA configuration. Also verify the paired platform with which the communication failure is reported is up and running BorderNet 4000 SBC software.
Platform Failover	HA	Major	This alarm is informational to the operator when the platform failed over and the fault/failure or the operation that resulted in this failover action.	This alarm is informational to the operator to indicate platform failover and its reason.

Name	Category	Severity	Description	Corrective Actions
Critical System Component Failed	HA	Critical	The system detects the failure of some critical system component in the platform that affects the system functionality. If this failure was detected on the platform that is serving the ACTIVE role, the system may decide to failover to the paired-platform if one is available. The system continues to provide the desired functionality.	The operator should review the available diagnostics to understand what component failed and the reason. If the issue persists the operator may contact support for further troubleshooting.
Platform Memory Size not As Expected	Hardware	Major	The BorderNet 4000 SBC system checks for the available physical memory on the platform during powerup checks. If memory is not as expected, the system raises this alarm.	Replace the bad memory card(s).
Power Supply Failed	Hardware		Indicates a power supply failure on the platform. The Alarm detail identifies the power supply that is detected as failed and the cause of the failure. Is the power supply is not present or not connected?	Check the power supply.
Fan Speed Sensor Reached Threshold	Hardware	Major	The Fan speed sensors detect that the fan failed or operating below configured fan speed thresholds indicating potential mechanical failures.	Check the platform fan.
Temperature Sensor Reached Threshold	Hardware	Major	The platform chassis inlet temperature is detected to be going above critical or non-recoverable thresholds.	Check the system hardware, fan and operating environment conditions and take adequate steps to provide proper system cooling.
RAID Device Degraded	Hardware	Major	The system detected the RAID degraded possibly due to HDD failure. The alarm details indicate which of the two HDD failed.	Check hard disks on the platform that is showing RAID degraded.
SDR File Transport Failure	SDR	Critical	The SDR file transport to the billing server failed.	Ensure that the SDR destination IP Address and directory name are

Name	Category	Severity	Description	Corrective Actions
				both correct. Make sure the network is working properly and the destination host has enough disk space.
Unsent SDR Files Accumulated	SDR	Critical	SDR files are not sent promptly.	Change the TCP parameters to increase the speed. Also, if SDR files are not compressed, you can change the setting to compress them.